



WEB APPLICATION FIREWALL

FortiWeb™ 5.2 Patch 4

CLI Reference



FortiWeb 5.2 Patch 4 CLI Reference

October 28, 2014

1st Edition

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare®, and FortiGuard® and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	http://docs.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forum
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction.....	23
Scope.....	23
Conventions.....	23
IP addresses	24
Cautions, notes, & tips.....	24
Typographic conventions	25
Command syntax.....	25
What's new.....	26
Using the CLI	34
Connecting to the CLI.....	34
Connecting to the CLI using a local console	34
Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget).....	35
Connecting to the CLI using SSH.....	37
Connecting to the CLI using Telnet	38
Command syntax.....	38
Terminology	39
Indentation	40
Notation	40
Subcommands.....	44
Table commands	44
Example of table commands	45
Field commands	46
Example of field commands	46
Permissions	47
Tips & tricks	50
Help.....	50
Shortcuts & key commands.....	50
Command abbreviation	51
Special characters	51
Language support & regular expressions	52
Screen paging.....	54
Baud rate	55
Editing the configuration file in a text editor	55
Administrative domains (ADOMs).....	57
Defining ADOMs	59
Assigning administrators to an ADOM.....	60

config	62
log alertemail	64
Syntax	64
Example	64
Related topics	64
log attack-log	65
Syntax	65
Example	66
Related topics	66
log custom-sensitive-rule	67
Syntax	67
Example	68
Related topics	69
log disk	70
Syntax	70
Example	71
Related topics	71
log email-policy	72
Syntax	72
Example	74
Related topics	75
log event-log	76
Syntax	76
Example	77
Related topics	77
log forti-analyzer	78
Syntax	78
Example	79
Related topics	79
log fortianalyzer-policy	80
Syntax	80
Example	80
Related topics	80
log memory	81
Syntax	81
Example	82
Related topics	82
log reports	83
Syntax	83
Example	90
Related topics	91

log sensitive	92
Syntax	92
Example	92
Related topics	92
log syslogd.....	93
Syntax	93
Example	94
log syslog-policy	95
Syntax	95
Example	95
Related topics	96
log traffic-log.....	97
Syntax	97
Example	98
Related topics	98
log trigger-policy	99
Syntax	99
Example	100
Related topics	100
router setting.....	101
Syntax	102
Example	102
Related topics	102
router static.....	103
Syntax	103
Example	104
Related topics	104
server-policy allow-hosts.....	105
Syntax	106
Example	107
Related topics	107
server-policy custom-application application-policy.....	108
Syntax	108
Example	108
Related topics	109
server-policy custom-application url-replacer.....	110
Syntax	111
Example	114
Related topics	114
server-policy dserver	115
Syntax	115
Example	115
Related topics	116

server-policy error-page	117
Syntax	117
Example	117
server-policy health	118
Syntax	118
Example	120
Related topics	120
server-policy http-content-routing-policy.....	121
Syntax	121
Example	123
Related topics	123
server-policy pattern custom-data-type.....	124
Syntax	124
Example	124
Related topics	124
server-policy pattern custom-global-white-list-group.....	125
Syntax	125
Example	126
Related topics	126
server-policy pattern custom-susp-url	127
Syntax	127
Example	127
Related topics	127
server-policy pattern custom-susp-url-rule.....	128
Syntax	128
Example	128
Related topics	129
server-policy pattern data-type-group	130
Syntax	130
Example	135
Related topics	136
server-policy pattern suspicious-url-rule.....	137
Syntax	137
Example	138
Related topics	139
server-policy policy.....	140
Syntax	141
Example	152
Related topics	153
server-policy pserver	154
Syntax	154
Example	154
Related topics	155

server-policy pservers	156
Syntax	156
Example	160
Related topics	161
server-policy service custom	162
Syntax	162
Example	162
Related topics	162
server-policy service predefined.....	163
Syntax	163
Example	163
Related topics	164
server-policy vserver.....	165
Syntax	165
Example	166
Related topics	166
system accprofile.....	167
Syntax	167
Example	169
Related topics	169
system admin.....	170
Syntax	170
Example	174
Related topics	174
system advanced.....	175
Syntax	175
Example	177
Related topics	177
system antivirus	178
Syntax	178
Related topics	179
system autoupdate override	180
Syntax	180
Related topics	180
system autoupdate schedule.....	181
Syntax	181
Example	182
Related topics	182
system autoupdate tunneling	183
Syntax	183
Example	183
Related topics	184

system backup	185
Syntax	185
Example	187
Related topics	188
system certificate ca	189
Syntax	189
Related topics	189
system certificate ca-group	190
Syntax	190
Example	190
Related topics	190
system certificate crt	191
Syntax	191
Related topics	191
system certificate intermediate-certificate	192
Syntax	192
Related topics	192
system certificate intermediate-certificate-group	193
Syntax	193
Related topics	193
system certificate local	194
Syntax	194
Example	195
Related topics	195
system certificate remote	196
Syntax	196
Related topics	196
system certificate verify	197
Syntax	197
Related topics	197
system conf-sync	198
Syntax	198
Related topics	199
system console	200
Syntax	200
Example	200
Related topics	200
system dns	201
Syntax	201
Example	201
Related topics	202
system dos-prevention	203
Syntax	203
Related topics	203

system fail-open	204
Syntax	205
Related topics	205
system global.....	206
Syntax	206
Example	211
Related topics	212
system ha.....	213
Syntax	214
Example	218
Related topics	219
system interface.....	220
Syntax	220
Example	226
Example	226
Related topics	226
system ip-detection	227
Syntax	227
Related topics	227
system network-option	228
Syntax	228
Related topics	228
system raid	229
Syntax	229
Example	229
Related topics	229
system settings.....	230
Syntax	232
Related topics	233
system snmp community.....	234
Syntax	234
Example	238
Related topics	238
system snmp sysinfo	239
Syntax	239
Example	240
Related topics	240
system v-zone.....	241
Syntax	241
Example	242
Related topics	242

user admin-usergrp	243
Syntax	243
Example	243
Related topics	244
user ldap-user	245
Syntax	245
Example	247
Related topics	248
user local-user	249
Syntax	249
Example	249
Related topics	250
user ntlm-user	251
Syntax	251
Example	251
Related topics	251
user radius-user	252
Syntax	252
Related topics	253
user user-group	254
Syntax	254
Example	255
Related topics	255
wad website	256
Syntax	256
Example	258
Related topics	259
waf allow-method-exceptions	260
Syntax	260
Example	261
Related topics	262
waf allow-method-policy	263
Syntax	263
Example	264
Related topics	264
waf application-layer-dos-prevention	265
Syntax	265
Example	266
Related topics	267
waf base-signature-disable	268
Syntax	268
Example	268
Related topics	268

waf brute-force-login	269
Syntax	269
Example	271
Related topics	271
waf custom-access policy	272
Syntax	272
Example	272
Related topics	272
waf custom-access rule.....	273
Syntax	273
Example	278
Related topics	279
waf custom-protection-group.....	280
Syntax	280
Example	280
Related topics	281
waf custom-protection-rule	282
Syntax	282
Example	285
Related topics	285
waf exclude-url	286
Syntax	286
Example	287
Related topics	287
waf file-compress-rule	288
Syntax	288
Example	289
Related topics	289
waf file-uncompress-rule	290
Syntax	290
Example	291
Related topics	291
waf file-upload-restriction-policy	292
Syntax	292
Related topics	294
waf file-upload-restriction-rule.....	295
Syntax	295
Example	297
Related topics	298
waf geo-block-list	299
Syntax	299
Example	300
Related topics	300

waf hidden-fields-protection.....	301
Syntax	301
Related topics	301
waf hidden-fields-rule	302
Syntax	302
Example	305
Related topics	306
waf http-authen http-authen-policy	307
Syntax	307
Example	308
Related topics	309
waf http-authen http-authen-rule	310
Syntax	310
Example	311
Related topics	312
waf http-connection-flood-check-rule	313
Syntax	313
Related topics	314
waf http-constraints-exceptions.....	315
Syntax	315
Example	317
Related topics	318
waf http-protocol-parameter-restriction	319
Syntax	319
Example	323
Related topics	323
waf http-request-flood-prevention-rule	324
Syntax	324
Example	326
Related topics	326
waf input-rule.....	327
Syntax	327
Example	330
Related topics	331
waf ip-intelligence.....	332
Syntax	332
Example	334
Related topics	334
waf ip-intelligence-exception.....	335
Syntax	335
Example	335
Related topics	335

waf ip-list	336
Syntax	336
Example	337
Related topics	338
waf layer4-access-limit-rule	339
Syntax	339
Example	341
Related topics	341
waf layer4-connection-flood-check-rule	342
Syntax	342
Example	343
Related topics	344
waf padding-oracle	345
Syntax	345
Example	348
Related topics	349
waf page-access-rule	350
Syntax	350
Example	352
Related topics	352
waf parameter-validation-rule	353
Syntax	353
Example	353
Related topics	354
waf signature	355
Syntax	356
Example	360
Related topics	361
waf site-publish-helper policy	362
Syntax	362
Example	362
Related topics	362
waf site-publish-helper rule	363
Syntax	364
Example	367
Related topics	367
waf start-pages	368
Syntax	368
Example	370
Related topics	371
waf url-access url-access-policy	372
Syntax	372
Example	372
Related topics	373

waf url-access url-access-rule.....	374
Syntax	374
Example	377
Related topics	378
waf url-rewrite url-rewrite-policy.....	379
Syntax	379
Related topics	379
waf url-rewrite url-rewrite-rule	380
Syntax	381
Related topics	386
waf web-protection-profile autolearning-profile	387
Syntax	387
Related topics	389
waf web-protection-profile inline-protection	390
Syntax	390
Related topics	400
waf web-cache-exception	401
Syntax	401
Related topics	402
waf web-cache-policy	403
Syntax	403
Related topics	405
waf web-protection-profile offline-protection.....	406
Syntax	406
Related topics	412
waf x-forwarded-for.....	413
Syntax	413
Example	415
wvs policy	417
Syntax	417
Example	418
Related topics	418
wvs profile.....	419
Syntax	419
Example	419
Example	419
Related topics	420
wvs schedule	421
Syntax	421
Example	422
Related topics	422

diagnose.....	423
debug.....	424
Syntax	425
Related topics	425
debug application autolearn	426
Syntax	426
Related topics	426
debug application detect	427
Syntax	427
Related topics	427
debug application dssl.....	428
Syntax	428
Related topics	428
debug application fds	429
Syntax	429
Related topics	429
debug application hasync.....	430
Syntax	430
Example	430
Related topics	432
debug application hatalk	433
Syntax	433
Example	433
Related topics	434
debug application http.....	435
Syntax	435
Related topics	435
debug application miglogd	436
Syntax	436
Related topics	436
debug application mulpattern.....	437
Syntax	437
Related topics	437
debug application proxy	438
Syntax	438
Related topics	438
debug application proxy-error	439
Syntax	439
Related topics	439
debug application snmp	440
Syntax	440
Related topics	440

debug application ssl.....	441
Syntax	441
Example	441
Related topics	441
debug application sysmon.....	442
Syntax	442
Related topics	442
debug application ustack	443
Syntax	443
Related topics	443
debug application waf-fds-update	444
Syntax	444
Related topics	444
debug cli	445
Syntax	445
Related topics	445
debug cmdb	446
Syntax	446
Related topics	446
debug comlog.....	447
Syntax	447
Related topics	447
debug console timestamp	448
Syntax	448
Related topics	448
debug crashlog	449
Syntax	449
Example	449
debug emerglog.....	450
Syntax	450
debug flow filter	451
Syntax	451
Related topics	452
debug flow reset	453
Syntax	453
Related topics	453
debug flow show module-process-detail	454
Syntax	454
Related topics	454
debug flow trace	455
Syntax	455
Example	455
Related topics	459

debug info	460
Syntax	460
Example	460
Related topics	461
debug init	462
Syntax	462
debug reset	463
Syntax	463
Related topics	463
debug upload	464
Syntax	464
Example	464
Related topics	464
hardware check	465
Syntax	465
Example	465
hardware cpu	466
Syntax	466
Example	466
Related topics	466
hardware fail-open	467
hardware harddisk	468
Syntax	468
Example	468
Related topics	468
hardware interrupts	469
Syntax	469
Example	469
Related topics	469
hardware logdisk info	470
Syntax	470
Example	470
Related topics	470
hardware mem	471
Syntax	471
Example	471
Related topics	472
hardware logdisk info	473
Syntax	473
Example	473
Related topics	473

hardware nic	474
Syntax	474
Example	474
Related topics	476
hardware raid list	477
Syntax	477
Example	477
Related topics	477
index	478
Syntax	478
Example	478
Related topics	478
log	479
Syntax	479
Example	479
Related topics	479
network arp	480
Syntax	480
Example	480
Related topics	480
network ip	481
Syntax	481
Example	481
Example	481
Related topics	482
network route	483
Syntax	483
Example	484
Example	484
Related topics	484
network rtcache	485
Syntax	485
Example	485
Example	485
Related topics	486
network sniffer	487
Syntax	488
Example	489
Example	490
Example	490
network tcp list	495
Syntax	495
Example	496
Related topics	496

network udp list	497
Syntax	497
Example	497
Related topics	497
policy	498
Syntax	498
Example	499
Related topics	499
system flash	500
Syntax	500
Example	500
Related topics	500
system ha mac	501
Syntax	501
Example	501
Related topics	501
system ha status	502
Syntax	502
Example	502
Related topics	502
system kill	503
Syntax	503
Related topics	503
system mount	504
Syntax	504
Example	504
Related topics	504
system top	505
Syntax	505
Example	505
Related topics	506
execute	507
backup cli-config	508
Syntax	508
Example	509
Related topics	509
backup full-config	510
Syntax	510
Example	510
Related topics	510
create-raid level	511
Syntax	511
Related topics	511

create-raid rebuild	512
Syntax	512
Example	512
Related topics	512
date	513
Syntax	513
Example	513
Related topics	513
db rebuild	514
Syntax	514
Related topics	514
factoryreset	515
Syntax	515
Related topics	515
formatlogdisk	516
Syntax	516
Related topics	516
ha disconnect	517
Syntax	517
Example	517
Related topics	518
ha manage	519
Syntax	519
Example	519
Related topics	519
ha synchronize	520
Syntax	520
Example	521
Related topics	521
ping	522
Syntax	522
Example	522
Example	522
Related topics	523
ping6	524
Syntax	524
Example	524
Related topics	524
ping-options	525
Syntax	525
Example	526
Related topics	526

ping6-options.....	527
Syntax	527
Example	528
Related topics	528
reboot	529
Syntax	529
Example	529
Related topics	529
restore config.....	530
Syntax	530
Example	530
Related topics	530
restore image.....	531
Syntax	531
Example	531
Related topics	531
restore secondary-image.....	532
Syntax	532
Example	532
Related topics	532
shutdown	533
Syntax	533
Example	533
Related topics	533
telnet	534
Syntax	534
Example	534
Related topics	534
telnettest	535
Syntax	535
Example	535
Related topics	536
time	537
Syntax	537
Example	537
Related topics	537
traceroute.....	538
Syntax	538
Example	538
Example	538
Example	539
Related topics	539
update-now.....	540
Syntax	540

get	541
router all	543
Syntax	543
Example	543
Related topics	543
system logged-users	544
Syntax	544
Example	544
Related topics	544
system performance	545
Syntax	545
Example	545
Related topics	545
system status.....	546
Syntax	546
Example	546
Related topics	546
show	547
Index	549

Introduction

Welcome, and thank you for selecting Fortinet products for your network protection.

Scope

This document describes how to use the command line interface (CLI) of the FortiWeb appliance. It assumes that you have already successfully installed the FortiWeb appliance and completed basic setup by following the instructions in the [FortiWeb Administration Guide](#).

At this stage:

- You have administrative access to the web UI and/or CLI.
- The FortiWeb appliance is integrated into your network.
- You have completed firmware updates, if applicable.
- The system time, DNS settings, administrator password, and network interfaces are configured.
- You have set the operation mode.
- You have configured basic logging.
- You have created at least one server policy.
- You have completed at least one phase of auto-learning to jump-start your configuration.

Once that basic installation is complete, you can use this document. This document explains how to use the CLI to:

- Update the FortiWeb appliance.
- Reconfigure features.
- Use advanced features, such as XML protection and reporting.
- Diagnose problems.

This document does **not** cover the web UI nor first-time setup. For that information, see the [FortiWeb Administration Guide](#).

Conventions

This document uses the conventions described in this section.

IP addresses

To avoid IP conflicts that would occur if you used examples in this document with public IP addresses that belong to a real organization, the IP addresses used in this document are fictional. They belong to the private IP address ranges defined by these RFCs.

RFC 1918: Address Allocation for Private Internets

<http://ietf.org/rfc/rfc1918.txt?number-1918>

RFC 5737: IPv4 Address Blocks Reserved for Documentation

<http://tools.ietf.org/html/rfc5737>

RFC 3849: IPv6 Address Prefix Reserved for Documentation

<http://tools.ietf.org/html/rfc3849>

For example, even though a real network's Internet-facing IP address would be routable on the public Internet, in this document's examples, the IP address would be shown as a non-Internet-routable IP such as 10.0.0.1, 192.168.0.1, or 172.16.0.1.

Cautions, notes, & tips

This document uses the following guidance and styles for notes, tips and cautions.



Warns you about procedures or feature behaviors that could have unexpected or undesirable results including loss of data or damage to equipment.



Highlights important, possibly unexpected but non-destructive, details about a feature's behavior.



Presents best practices, troubleshooting, performance tips, or alternative methods.

Typographic conventions

Table 1: Typographical conventions in this document

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FortiWeb# diagnose hardware logdisk info disk number: 1 disk[0] size: 31.46GB raid level: no raid exists partition number: 1 mount status: read-write</pre>
Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	https://support.fortinet.com
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <i>VPN > IPSEC > Auto Key (IKE)</i> .
Publication	For details, see the <i>FortiScan Administration Guide</i> .

Command syntax

The CLI requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

For command syntax conventions such as braces, brackets, and command constraints such as `<address_ipv4>`, see “[Notation](#)” on page 40.

What's new

The tables below list commands which have changed since FortiWeb 5.0 Patch 4, including new commands, syntax changes, and new setting options.

FortiWeb 5.2 Patch 4

Command	Change
<code>config system advanced</code>	
<code>set no-ssl3 {enable disable}</code>	New. You can now prevent clients from using SSL 3.0 to connect to back-end servers.
<code>config system global</code>	
<code>set no-ssl3 {enable disable}</code>	New. You can now prevent connections to the web UI via SSL 3.0.

FortiWeb 5.2

Command	Change
<code>config system certificate ca</code> <code>config system certificate ca-group</code> <code>config system certificate crl</code> <code>config system certificate intermediate-certificate</code> <code>config system certificate intermediate-certificate-group</code> <code>config system certificate local</code> <code>config system certificate remote</code> <code>config system certificate verify</code>	Changed. When ADOMs are enabled, you now perform certificate configuration under <code>config vdom</code> instead of <code>config global</code> . This allows each administrative domain to have its own certificates and certificate-related settings. See “Administrative domains (ADOMs)” on page 57.
<code>config system interface</code> <code>edit <interface_name></code> <code>set allowaccess {http https ping snmp ssh telnet}</code> <code>set ip6-allowaccess {http https ping snmp ssh telnet}</code>	Changed. You can now configure administrative access for VLAN subinterfaces.
<code>config waf url-access</code> <code>url-access-rule</code> <code>edit url-access-rule-name <url-access-rule_name></code> <code>config match condition</code> <code>edit <entry_index></code> <code>set sip-address-value <client_ip></code>	Changed. You can now specify either a single IP address or an IP address range.

Command	Change
<pre>config waf ip-list edit <ip-list_name> config members edit <entry_index> set ip <client_ip></pre>	<p>Changed. You can now specify either a single IP address or an IP address range.</p>
<pre>config waf custom-access rule edit <custom-access_name> config http-transaction edit <entry_index> set http-transaction-timeout <timeout_int> config response-code edit <entry_index> set response-code-min <response-code_int> set response-code-max <response-code_int> config packet-interval edit packet-interval-timeout <timeout_int> config signature-class edit {010000000 020000000 030000000 040000000 050000000 060000000 090000000} set status {enable disable} config occurrence edit <entry_index> set occurrence-num <occurrence_int> set within <within_int> set traced-by {Source-IP User}</pre>	<p>New. Additional filter types include:</p> <ul style="list-style-type: none"> • Transaction and packet interval timeout • HTTP response code • URL • Attack signature violation

FortiWeb 5.1 Patch 3

Command	Change
<pre>config waf web-cache-exception edit <web-cache-exception_rule_name> config exception-list edit <entry_index> set host-status {enable disable} set host <host_str> set url-type {plain regular} set url-pattern <url-pattern_str> set cookie-name <cookie-name_str></pre>	New. Allows you to specify exceptions to caching of responses from back-end servers.
<pre>config waf web-cache-policy edit <web-cache-policy_rule_name> set cache-buffer-size <cache-size_int> set max-cached-page-size <page-size_int> set default-cache-timeout <cache-timeout_int> set exception <web-cache-exception_name> config url-match-list edit <entry_index> set host-status {enable disable} set host <host_str> set url-type {plain regular} set url-pattern <url-pattern_str></pre>	New. Allows you enable caching of responses from back-end servers.
<pre>config waf web-protection-profile inline-protection set web-cache-policy <web-cache-policy_name></pre>	New. Option to add caching policies to the profile.

FortiWeb 5.1 Patch 2

Command	Change
<pre>config log attack-log set packet-log {allow-robot anti-virus-detection cookie-poison custom-access custom-protection-rule hidden-fields-failed http-protocol-constraints illegal-file-type illegal-xml-format ip-intelligence padding-oracle parameter-rule-failed signature-detection}</pre>	Changed. Added options to log padding oracle attacks.
<pre>config server-policy http-content-routing-policy set cookie-name <cookie-name_str> set cookie-type {Regular-expression Simple-string} set cookie-value <cookie-val_str> set is-essential {yes no}</pre>	New. FortiWeb can now load balance traffic based on cookies embedded by your back-end servers.

Command	Change
<pre>config waf padding-oracle edit <padding-oracle_rule_name> set action {alert alert_deny block-period} set block-period <block-period_int> set severity {High Medium Low} set trigger <trigger-policy_name> config protected-url-list edit <entry_index> set host-status {enable disable} set host <host_str> set url-type {plain regular} set protected-url <protected-url_str> set target {cookie parameter url} config waf web-protection-profile inline-protection set padding-oracle <rule_name> config waf web-protection-profile offline-protection set padding-oracle <rule_name></pre>	<p>New. Allows you to create a policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS.</p> <p>New. Option to add padding oracle attacks configuration to profile.</p> <p>New. Option to add padding oracle attacks configuration to profile.</p>

FortiWeb 5.1 Patch 1

No design changes. Bug fixes only.

FortiWeb 5.1

IPv6 is not supported by some features. For details, see the [FortiWeb Administration Guide](#).

Command	Change
<pre>config log attack-log set packet-log {allow-robot anti-virus-detection cookie-poison custom-access custom-protection-rule hidden-fields-failed http-protocol-constraints illegal-file-type illegal-xml-format ip-intelligence padding-oracle parameter-rule-failed signature-detection}</pre>	Changed. Added options to log illegal file types for uploads and cookie poisoning.
<pre>config server-policy policy edit <policy_name> set hsts-header {enable disable} set hsts-max-age <timeout_int> set http-pipeline {enable disable}</pre>	New. Enforces subsequent use of HTTPS only. New. Enables HTTP pipelining.
<pre>config server-policy pservers edit <server-farm_name> config pserver-list edit <entry_index> set hsts-header {enable disable} set hsts-max-age <timeout_int></pre>	New. Enforces subsequent use of HTTPS only.
<pre>config system admin edit <administrator_name> set accprofile <access-profile_name> set accprofile-override {enable disable} set domains <adom_name></pre>	Changed. Now can be overridden by RADIUS VSA FortiWeb-Access-Profile. New. Supports overriding the locally assigned access profile via RADIUS VSA. New. Assigns the administrator account to an administrative domain (ADOM).

Command	Change
<code>config system global</code>	
<code>set adom-admin {enable disable}</code>	New. Enables administrative domains (ADOMs). See also “Administrative domains (ADOMs)” on page 57.

FortiWeb 5.0 Patch 4

Command	Change
<code>config server-policy pattern</code>	
<code>data-type-group</code>	
<code>edit <data-type-group_name></code>	
<code>config type-list</code>	
<code>edit <entry_index></code>	
<code>set data-type {Address Canadian_Post_code Canadian_Province_Name Canadian_SIN China_Post_Code Country_Name Credit_Card_Number Danmark_Postalcode Dates_and_Times Email GPA GUID ip_address Indian_Vehicle_Number Italian_mobile_phone Kuwait_Civil_ID L1_Password L2_Password Markup_or_Code Microsoft_product_key NINO Netherlands_Postcode Num personal_name Phone Quebec_Postal_Code String Swedish_personal_number Swedish_Postalcode UAE_land_phone UK_Bank_code UK_postcode US_SSN US_State_Name US_Street_Address US_Zip_Code Unix_device_name Uri Windows_file_name}</code>	New options Swedish_Postalcode, Italian_mobile_phone, and Quebec_Postal_Code match postal codes for Quebec, Canada and Sweden as well as Italian mobile phone numbers.
<code>config system advanced</code>	

Command	Change
<pre> set max-http-argbuf-length {8k-cache 12k-cache 32k-cache 64k-cache} </pre>	New option 64k-cache.
<pre> config system network-option set tcp-timestamp {enable disable} set tcp-tw-recycle {enable disable} </pre>	New. Configures inclusion and validation of the TCP timestamp and connection recycling.
<pre> config waf input-rule edit <input-rule_name> config rule-list edit <entry_index> set data-type <predefined_name> </pre>	New options Swedish_Postalcode, Italian_mobile_phone, and Quebec_Postal_Code match postal codes for Quebec, Canada and Sweden as well as Italian mobile phone numbers.
<pre> config waf site-publish-helper rule edit <site-publish-rule_name> set req-type {plain regular} set published-site <host_fqdn> config waf site-publish-helper rule </pre>	New. To support quickly publishing the same web applications for multiple subdomains, regular expression support has been added.

Using the CLI

The command line interface (CLI) is an alternative to the web UI.

You can use either interface or both to configure the FortiWeb appliance. In the web UI, you use buttons, icons, and forms, while, in the CLI, you either type text commands or upload batches of commands from a text file, like a configuration script.

If you are new to Fortinet products, or if you are new to the CLI, this section can help you to become familiar.

Connecting to the CLI

You can access the CLI in two ways:

- **Locally** — Connect your computer, terminal server, or console directly to the FortiWeb appliance's console port.
- **Through the network** — Connect your computer through any network attached to one of the FortiWeb appliance's network ports. To connect using an Secure Shell (SSH) or Telnet client, enable the network interface for Telnet or SSH administrative access. Enable HTTP/HTTPS administrative access to connect using the *CLI Console* widget in the web UI.

Local access is required in some cases.

- If you are installing your FortiWeb appliance for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local console connection. See the [FortiWeb Administration Guide](#).
- Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until **after** the boot process completes, and therefore local CLI access is the only viable option.

Before you can access the CLI through the network, you usually must enable SSH and/or HTTP/HTTPS and/or Telnet on the network interface through which you will access the CLI.

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiWeb appliance, using its DB-9 console port.

Requirements

- a computer with an available serial communications (COM) port
- the RJ-45-to-DB-9 or null modem cable included in your FortiWeb package
- terminal emulation software such as [PuTTY](#)



The following procedure describes connection using PuTTY software; steps may vary with other terminal emulators.

To connect to the CLI using a local console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiWeb appliance's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start [PuTTY](#).
3. In the *Category* tree on the left, go to *Connection > Serial* and configure the following:

Serial line to connect to	COM1 (or, if your computer has multiple serial ports, the name of the connected serial port)
Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow control	None
4. In the *Category* tree on the left, go to *Session* (**not** the sub-node, *Logging*) and from *Connection type*, select *Serial*.
5. Click *Open*.
6. Press the Enter key to initiate a connection.
The login prompt appears.
7. Type a valid administrator account name (such as `admin`) then press Enter.
8. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)
The CLI displays the following text, followed by a command line prompt:
`Welcome!`
You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see [“Enabling access to the CLI through the network \(SSH or Telnet or CLI Console widget\)”](#) on page 35.

Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget)

SSH, Telnet, or *CLI Console* widget (via the web UI) access to the CLI requires connecting your computer to the FortiWeb appliance using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.



If you do not want to use an SSH/Telnet client and you have access to the web UI, you can alternatively access the CLI through the network using the *CLI Console* widget in the web UI. For details, see the [FortiWeb Administration Guide](#).

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is **not** connected directly or through a switch, you must also configure the FortiWeb appliance with a static route to a router that can forward packets from the FortiWeb appliance to your computer (see [“config router static”](#) on page 103).

You can do this using either:

- a local console connection (see the following procedure)
- the web UI (see the [FortiWeb Administration Guide](#))

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as [PuTTY](#)
- the RJ-45-to-DB-9 or null modem cable included in your FortiWeb package
- a crossover Ethernet cable (if connecting directly) or straight-through Ethernet cable (if connecting through a switch or router)
- prior configuration of the operating mode, network interface, and static route (for details, see the [FortiWeb Administration Guide](#)).

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiWeb appliance's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiWeb appliance.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI. For details, see [“Connecting to the CLI using a local console” on page 34](#).

4. Enter the following commands:

```
config system interface
    edit <interface_name>
        set allowaccess {http https ping snmp ssh telnet}
    end
```

where:

- <interface_name> is the name of the network interface associated with the physical network port, such as `port1`
- {http https ping snmp ssh telnet} is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`; omit protocols that you do not want to permit

For example, to exclude HTTP, SNMP, and Telnet, and allow only HTTPS, ICMP ECHO (ping), and SSH administrative access on `port1`:

```
config system interface
    edit "port1"
        set allowaccess ping https ssh
    next
end
```



Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

5. To confirm the configuration, enter the command to view the access settings for the interface.

```
show system interface <interface_name>
```

The CLI displays the settings, including the management access settings, for the interface.

6. If you will be connecting indirectly, through one or more routers or firewalls, configure the appliance with at least one static route so that replies from the CLI can reach your client. See [“config router static” on page 103](#).

To connect to the CLI through the network interface, see [“Connecting to the CLI using SSH” on page 37](#) or [“Connecting to the CLI using Telnet” on page 38](#).

Connecting to the CLI using SSH

Once you configure the FortiWeb appliance to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. Supported SSH protocol versions, ciphers, and bit strengths vary by whether or not you have enabled FIPS-CC mode or are using a low encryption (LENC) version, but generally include SSH version 2 with AES-128, 3DES, Blowfish, and SHA-1.

Requirements

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- a FortiWeb network interface configured to accept SSH connections (see [“Enabling access to the CLI through the network \(SSH or Telnet or CLI Console widget\)” on page 35](#))
- an SSH client such as [PuTTY](#)

To connect to the CLI using SSH

1. On your management computer, start [PuTTY](#).
Initially, the *Session* category of settings is displayed.
2. In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled SSH administrative access.
3. In *Port*, type 22.
4. From *Connection type*, select SSH.
5. Click *Open*.

The SSH client connects to the FortiWeb appliance.

The SSH client may display a warning if this is the first time you are connecting to the FortiWeb appliance and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiWeb appliance but it used a different IP address or SSH key. If your management computer is directly connected to the FortiWeb appliance with no network hosts between them, this is normal.

6. Click Yes to verify the fingerprint and accept the FortiWeb appliance’s SSH key. You will not be able to log in until you have accepted the key.

The CLI displays a login prompt.

7. Type a valid administrator account name (such as `admin`) and press Enter.
8. Type the password for this administrator account and press Enter.



If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The FortiWeb appliance displays a command prompt (its host name followed by a #) . You can now enter CLI commands.

Connecting to the CLI using Telnet

Once the FortiWeb appliance is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.



Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Requirements

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- a FortiWeb network interface configured to accept Telnet connections (see [“Enabling access to the CLI through the network \(SSH or Telnet or CLI Console widget\)”](#) on page 35)
- terminal emulation software such as [PuTTY](#)

To connect to the CLI using Telnet

1. On your management computer, start [PuTTY](#).
2. In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled Telnet administrative access.
3. In *Port*, type 23.
4. From *Connection type*, select *Telnet*.
5. Click *Open*.
6. Type a valid administrator account name (such as `admin`) and press Enter.
7. Type the password for this administrator account and press Enter.



If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The CLI displays a command line prompt (by default, its host name followed by a #). You can now enter CLI commands.

Command syntax

When entering a command, the CLI requires that you use valid syntax and conform to expected input constraints. It will reject invalid commands.

For example, if you do not type the entire object that will receive the action of a command operator such as `config`, the CLI will return an error message such as:

```
Command fail. CLI parsing error
```

Fortinet documentation uses the following conventions to describe valid command syntax.

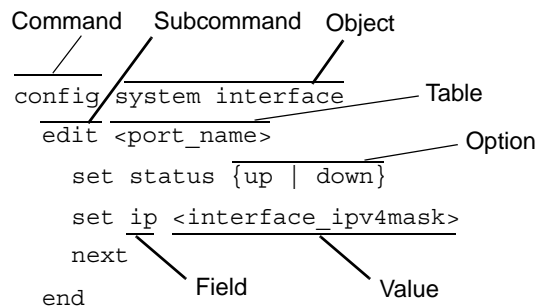
Terminology

Each command line consists of a command word followed by words for the configuration data or other specific item that the command uses or affects, for example:

```
get system admin
```

Fortinet documentation uses terms in [Figure 1](#) to describe the function of each word in the command line.

Figure 1: Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiWeb appliance should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that you terminate by pressing the Enter key, it forms a command line. Exceptions include multi-line command lines, which can be entered using an escape sequence. (See [“Shortcuts & key commands” on page 50.](#))

Valid command lines must be unambiguous if abbreviated. (See [“Command abbreviation” on page 51.](#)) Optional words or other command line permutations are indicated by syntax notation. (See [“Notation” on page 40.](#))



This CLI Reference is organized alphabetically by object for the `config` command, and by the name of the command for remaining top-level commands.

If you do not enter a known command, the CLI will return an error message such as:

```
Unknown action 0
```

- **subcommand** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable subcommands are available to you until you exit the scope of the command, or until you descend an additional level into another subcommand. Indentation is used to indicate levels of nested commands. (See [“Indentation” on page 40.](#))

Not all top-level commands have subcommands. Available subcommands vary by their containing scope. (See [“Subcommands” on page 44.](#))

- **object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets that each have a name or number, such as an administrator account, policy, or network interface. These named or

numbered sets are sometimes referenced by other parts of the configuration that use them. (See [“Notation” on page 40.](#))

- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiWeb appliance will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually the configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See [“Notation” on page 40.](#))
- **option** — A kind of value that must be one or more words from a fixed set of options. (See [“Notation” on page 40.](#))

Indentation

Indentation indicates levels of nested commands, which indicate what other subcommands are available from within the scope.

For example, the `edit` subcommand is available only within a command that affects tables, and the `next` subcommand is available only from within the `edit` subcommand:

```
config system interface
  edit port1
    set status up
  next
end
```

For information about available subcommands, see [“Subcommands” on page 44.](#)

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.



If you do not use the expected data type, the CLI returns an error message such as:

```
object set operator error, -4003 discard the setting
The request URL must start with "/" and without domain name.
```

or:

```
invalid unsigned integer value :-:
```

```
value parse error before '-'
```

```
Input value is invalid.
```

and may either **reject** or **discard** your settings instead of saving them when you type `end`.

Table 2: Command syntax notation

Convention	Description
Square brackets []	<p>A non-required (optional) word or words. For example:</p> <pre>[verbose {1 2 3}]</pre> <p>indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as:</p> <pre>verbose 3</pre>
Curly braces { }	<p>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces.</p> <p>You must enter at least one of the options, unless the set of options is surrounded by square brackets [].</p>

Table 2: Command syntax notation

Convention		Description
	Options delimited by vertical bars	Mutually exclusive options. For example: <code>{enable disable}</code> indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
	Options delimited by spaces	Non-mutually exclusive options. For example: <code>{http https ping snmp ssh telnet}</code> indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: <code>ping https ssh</code> Note: To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type: <code>ping https snmp ssh</code> If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Table 2: Command syntax notation

Convention	Description
Angle brackets < >	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (<code>_</code>) and suffix that indicates the valid data type. For example:</p> <pre><retries_int></pre> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> • <code><xxx_name></code> — A name referring to another part of the configuration, such as <code>policy_A</code>. • <code><xxx_index></code> — An index number referring to another part of the configuration, such as 0 for the first static route. • <code><xxx_pattern></code> — A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all e-mail addresses ending in <code>@example.com</code>. • <code><xxx_fqdn></code> — A fully qualified domain name (FQDN), such as <code>mail.example.com</code>. • <code><xxx_email></code> — An email address, such as <code>admin@mail.example.com</code>. • <code><xxx_url></code> — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet.com/</code>. • <code><xxx_ipv4></code> — An IPv4 address, such as <code>192.168.1.99</code>. • <code><xxx_v4mask></code> — A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>. • <code><xxx_ipv4mask></code> — A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>. • <code><xxx_ipv4/mask></code> — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>. • <code><xxx_ipv6></code> — A colon (<code>:</code>)-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>. • <code><xxx_v6mask></code> — An IPv6 netmask, such as <code>/96</code>. • <code><xxx_ipv6mask></code> — An IPv6 address and netmask separated by a space. • <code><xxx_str></code> — A string of characters that is not another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See “Special characters” on page 51. • <code><xxx_int></code> — An integer number that is not another data type, such as 15 for the number of minutes.

Subcommands

Once you connect to the CLI, you can enter commands.

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects, for example:

```
get system admin
```

Subcommands are available from within the scope of some commands. When you enter a subcommand level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin) #
```

Applicable subcommands are available to you until you exit the scope of the command, or until you descend an additional level into another subcommand.

For example, the `edit` subcommand is available only within a command that affects tables; the `next` subcommand is available only from within the `edit` subcommand:

```
config system interface
  edit port1
    set status up
  next
end
```

Available subcommands vary by command. From a command prompt within `config`, two types of subcommands might become available:

- commands that affect fields (see [“Field commands” on page 46](#))
- commands that affect tables (see [“Table commands” on page 44](#))



Subcommand scope is indicated in this CLI Reference by indentation. See [“Indentation” on page 40](#).

Syntax examples for each top-level command in this CLI Reference do not show all available subcommands. However, when nested scope is demonstrated, you should assume that subcommands applicable for that level of scope are available.

Table commands

Table 3: Commands for tables

<code>delete</code> <code><table_name></code>	<p>Remove a table from the current object.</p> <p>For example, in <code>config system admin</code>, you could delete an administrator account named <code>newadmin</code> by typing <code>delete newadmin</code> and pressing Enter. This deletes <code>newadmin</code> and all its fields, such as <code>newadmin</code>'s first-name and email-address.</p> <p><code>delete</code> is only available within objects containing tables.</p>
--	--

Table 3: Commands for tables

<i>edit</i> <i><table_name></i>	<p>Create or edit a table in the current object.</p> <p>For example, in <code>config system admin</code>:</p> <ul style="list-style-type: none"> edit the settings for the default <code>admin</code> administrator account by typing <code>edit admin</code>. add a new administrator account with the name <code>newadmin</code> and edit <code>newadmin</code>'s settings by typing <code>edit newadmin</code>. <p><code>edit</code> is an interactive subcommand: further subcommands are available from within <code>edit</code>.</p> <p><code>edit</code> changes the prompt to reflect the table you are currently editing.</p> <p><code>edit</code> is only available within objects containing tables.</p>
<i>end</i>	<p>Save the changes to the current object and exit the <code>config</code> command. This returns you to the top-level command prompt.</p>
<i>get</i>	<p>List the configuration of the current object or table.</p> <ul style="list-style-type: none"> In objects, <code>get</code> lists the table names (if present), or fields and their values. In a table, <code>get</code> lists the fields and their values. <p>For more information on <code>get</code> commands, see “get” on page 541.</p>
<i>purge</i>	<p>Remove all tables in the current object.</p> <p>For example, in <code>config user local-user</code>, you could type <code>get</code> to see the list of all local user names, then type <code>purge</code> and then <code>y</code> to confirm that you want to delete all users.</p> <p><code>purge</code> is only available for objects containing tables.</p> <p>Caution: Back up the FortiWeb appliance before performing a purge because it cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see “execute backup cli-config” on page 508.</p> <p>Caution: Do not purge <code>system interface</code> or <code>system admin</code> tables. This can result in being unable to connect or log in, requiring the FortiWeb appliance to be formatted and restored.</p>
<i>show</i>	<p>Display changes to the default configuration. Changes are listed in the form of configuration commands.</p> <p>For more information on <code>show</code> commands, see “show” on page 547.</p>

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1) #
```

Field commands

Table 4: Commands for fields

abort	Exit both the <code>edit</code> and/or <code>config</code> commands without saving the fields.
end	Save the changes made to the current table or object fields, and exit the <code>config</code> command. (To exit without saving, use <code>abort</code> instead.)
get	List the configuration of the current object or table. <ul style="list-style-type: none">• In objects, <code>get</code> lists the table names (if present), or fields and their values.• In a table, <code>get</code> lists the fields and their values.
next	Save the changes you have made in the current table's fields, and exit the <code>edit</code> command to the object prompt. (To save and exit completely to the root prompt, use <code>end</code> instead.) <code>next</code> is useful when you want to create or edit several tables in the same object, without leaving and re-entering the <code>config</code> command each time. <code>next</code> is only available from a table prompt; it is not available from an object prompt.
set <field_name> <value>	Set a field's value. For example, in <code>config system admin</code> , after typing <code>edit admin</code> , you could type <code>set password newpass</code> to change the password of the admin administrator to <code>newpass</code> . Note: When using <code>set</code> to change a field containing a space-delimited list, type the whole new list. For example, <code>set <field> <new-value></code> will replace the list with the <code><new-value></code> rather than appending <code><new-value></code> to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unset <field_name>	Reset the table or object's fields to default values. For example, in <code>config system admin</code> , after typing <code>edit admin</code> , typing <code>unset password</code> resets the password of the admin administrator account to the default (in this case, no password).

Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Depending on the account that you use to log in to the FortiWeb appliance, you may not have complete access to all CLI commands or areas of the web UI.

Access profiles control which commands and areas an administrator account can access.

Access profiles assign either:

- *Read* (view access)
- *Write* (change and execute access)
- both *Read* and *Write*
- no access

to each area of the FortiWeb software. For more information on configuring the access profile for an administrator account to use, see [“config system accprofile” on page 167](#).

Table 5: Areas of control in access profiles

Access profile setting	Grants access to*	
Admin Users admingrp	System > Admin ... except Settings config system admin config system accprofile	Web UI
		CLI
Auth Users authusergrp	User ... config user ...	Web UI
		CLI
Autolearn Configuration learngrp	Auto Learn > Auto Learn Profile > Auto Learn Profile config server-policy custom-application ... config waf web-protection-profile autolearning-profile Note: Because generating an auto-learning profile also generates its required components, this area also confers <i>Write</i> permission to those components in the <i>Web Protection Configuration/wafgrp</i> area.	Web UI
		CLI
Log & Report loggrp	Log&Report ... config log ... execute formatlogdisk	Web UI
		CLI
Maintenance mntgrp	System > Maintenance except System Time tab diagnose system ... execute backup ... execute factoryreset execute reboot execute restore ... execute shutdown diagnose system flash ...	Web UI
		CLI

Table 5: Areas of control in access profiles

Access profile setting	Grants access to*	
<i>Network Configuration</i> netgrp	System > Network ... config router ... config system interface config system dns config system v-zone diagnose network ... except sniffer ...	Web UI
		CLI
<i>System Configuration</i> sysgrp	System ... except Network, Admin, and Maintenance tabs config system except accprofile, admin, dns, interface, and v-zone diagnose hardware ... diagnose network sniffer ... diagnose system ... except flash ... execute date ... execute ha ... execute ping ... execute ping-option ... execute traceroute ... execute time ...	Web UI
		CLI
<i>Server Policy Configuration</i> traroutegrp	Policy > Server Policy ... Server Objects ... Application Delivery ... config server-policy ... except custom-application ... config waf file-compress-rule config waf file-uncompress-rule config waf http-authen ... config waf url-rewrite ... diagnose policy ...	Web UI
		CLI
<i>Web Anti-Defacement Management</i> wadgrp	Web Anti-Defacement ... config wad ...	Web UI
		CLI

Table 5: Areas of control in access profiles

Access profile setting	Grants access to*	
<i>Web Protection Configuration</i>	<i>Policy > Web Protection ...</i> <i>Web Protection ...</i> <i>DoS Protection ...</i>	Web UI
wafgrp	config system dos-prevention config waf except: <ul style="list-style-type: none"> • config waf file-compress-rule • config waf file-uncompress-rule • config waf http-authen ... • config waf url-rewrite ... • config waf web-custom-robot • config waf web-protection-profile autolearning-profile • config waf web-robot • config waf x-forwarded-for 	CLI
<i>Web Vulnerability Scan Configuration</i>	<i>Web Vulnerability Scan ...</i>	Web UI
wvsgrp	config wvs ...	CLI

* For each config command, there is an equivalent get/show command, unless otherwise noted.

config access requires write permission.

get/show access requires read permission.

Unlike other administrator accounts, the administrator account named `admin` exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiWeb configuration options, including viewing and changing **all** other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.



Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiWeb appliance.

For complete access to all commands, you must log in with the administrator account named `admin`.

Tips & tricks

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

This section includes:

- [Help](#)
- [Shortcuts & key commands](#)
- [Command abbreviation](#)
- [Special characters](#)
- [Language support & regular expressions](#)
- [Screen paging](#)
- [Baud rate](#)
- [Editing the configuration file in a text editor](#)

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each.
- Press the question mark (?) key after a command keyword to display a list of the objects available with that command and a description of each.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts & key commands

Table 6: Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A

Table 6: Shortcuts and key commands

Action	Keys
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as <code>config</code> or <code>edit</code> , this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters. For example, the command `get system status` could be abbreviated to:

```
g sy st
```

If you enter an ambiguous command, the CLI returns an error message such as:

```
ambiguous command before 's'
Value conflicts with system settings.
```

Special characters

Special characters `<`, `>`, `(`, `)`, `#`, `'`, and `"` are usually not permitted in CLI. If you use them, the CLI will often return an error message such as:

```
The string contains XSS vulnerability characters
```

```
value parse error before '%^@'
Input not as expected.
```

Some may be enclosed in quotes or preceded with a backslash (\) character.

Table 7: Entering special characters

Character	Key
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: "Security Administrator". Enclose the string in single quotes: 'Security Administrator'. Precede the space with a backslash: Security\ Administrator.

Table 7: Entering special characters

Character	Key
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Language support & regular expressions

Languages currently supported by the CLI interface include:

- English
- Japanese
- simplified Chinese
- traditional Chinese

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice.

For example, the host name must not contain special characters, and so the web UI and CLI will not accept most symbols and other non-ASCII encoded characters as input when configuring the host name. This means that languages other than English often are not supported. However, some configuration items, such as names and comments, may be able to use the language of your choice.

To use other languages in those cases, you must use the correct encoding.

The FortiWeb appliance stores the input using Unicode UTF-8 encoding, but it is not normalized from other encodings into UTF-8 before stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.

For example, with Shift-JIS, backslashes (\) could be inadvertently interpreted as yen symbols (¥) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients



HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

To configure your FortiWeb appliance using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet or SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.



If you choose to configure parts of the FortiWeb appliance using non-ASCII characters, verify that all systems interacting with the FortiWeb appliance also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of your web browser or Telnet or SSH client while you work.

Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web UI or CLI. Exceptions include items such as regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiWeb appliance receives.

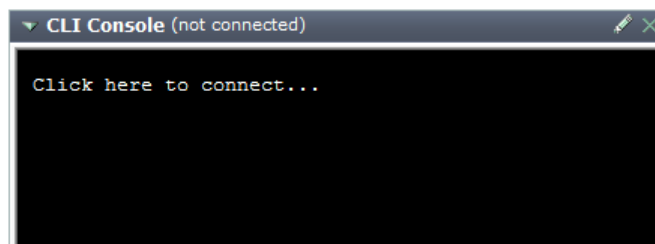
To enter non-ASCII characters in the CLI Console widget

1. On your management computer, start your web browser and go to the URL for the FortiWeb appliance's web UI.
2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiWeb appliance.
4. Go to *System > Status > Status*.
5. In title bar of the *CLI Console* widget, click the *Edit* icon.
The *Console Preferences* dialog appears in a pop-up window.
6. Enable *Use external command input box*.
7. Click *OK*.

The *Command* field appears below the usual input and display area of the *CLI Console* widget.

8. In *Command*, type a command.

Figure 2: CLI Console widget



9. Press Enter.

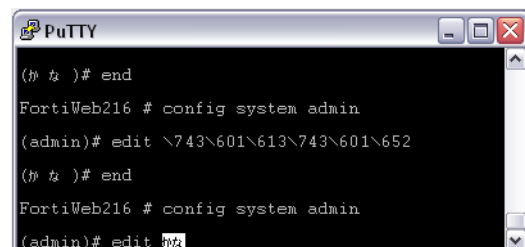
In the display area, the *CLI Console* widget displays your previous command interpreted into its character code equivalent, such as:

```
edit \743\601\613\743\601\652
and the command's output.
```

To enter non-ASCII characters in a Telnet or SSH client

1. On your management computer, start your Telnet or SSH client.
2. Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding the encoding.
Support for sending and receiving international characters varies by each Telnet or SSH client. Consult the documentation for your Telnet or SSH client.
3. Log in to the FortiWeb appliance.
4. At the command prompt, type your command and press Enter.

Figure 3: Entering encoded characters (PuTTY)



You may need to surround words that use encoded characters with single quotes (').

Depending on your Telnet or SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5. The CLI displays your previous command and its output.

Screen paging

When output spans multiple pages, you can configure the CLI to pause after each page. When the display pauses, the last line displays `--More--`. You can then either:

- Press the spacebar to display the next page.
- Type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause after each full screen:

```
config system console
    set output more
end
```

For more information, see [“config system console” on page 200](#).

Baud rate

You can change the default baud rate of the local console connection. For more information, see [“config system console” on page 200](#).

Editing the configuration file in a text editor

Editing the configuration file with a plain text editor can be time-saving if:

- you have many changes to make,
- are not sure where the setting is in the CLI, and/or
- own several FortiWeb appliances

This is true especially if your plain text editor provides advanced features such as regular expressions for find-and-replace, or batch changes across multiple files. Several free text editors are available with these features, such as [Text Wrangler](#) and [Notepad++](#).



Do **not** use a rich text editor such as Microsoft Word. Rich text editors insert special characters into the file in order to apply formatting, which may corrupt the configuration file.

To edit the configuration on your computer

1. Use [execute backup cli-config](#) or [execute backup full-config](#) to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.



Do not edit the first line. The first lines of the configuration file (preceded by a # character) contains information about the firmware version and FortiWeb model. If you change the model number, the FortiWeb appliance will reject the configuration file when you attempt to restore it.

3. Use [execute restore config](#) to upload the modified configuration file back to the FortiWeb appliance.

The FortiWeb appliance downloads the configuration file and checks that the model information is correct. If it is, the FortiWeb appliance loads the configuration file and checks each command for errors. If a command is invalid, the FortiWeb appliance ignores the command. If the configuration file is valid, the FortiWeb appliance restarts and loads the new configuration.

Administrative domains (ADOMs)

Administrative domains (ADOMs) enable the `admin` administrator to constrain other FortiWeb administrators' access privileges to a subset of policies and protected host names. This can be useful for large enterprises and multi-tenant deployments such as web hosting.

ADOMs are **not** enabled by default. Enabling and configuring administrative domains can only be performed by the `admin` administrator.

Enabling ADOMs alters the structure of and the available functions in the GUI and CLI, according to whether or not you are logging in as the `admin` administrator, and, if you are **not** logging in as the `admin` administrator, the administrator account's assigned access profile.

Table 8: Differences between administrator accounts when ADOMs are enabled

	<code>admin</code> administrator account	Other administrators
Access to config global	Yes	No
Can create administrator accounts	Yes	No
Can create & enter all ADOMs	Yes	No

- If ADOMs are enabled and you log in as `admin`, a superset of the typical CLI commands appear, allowing unrestricted access and ADOM configuration.
`config global` contains settings used by the FortiWeb itself and settings shared by ADOMs, such as RAID and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.
- If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, policies, servers, and LDAP queries specific to your ADOM. You cannot access global configuration settings, or enter other ADOMs.
By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all policies and servers. By creating ADOMs that contain a subset of policies and servers, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiWeb's total protected servers.

The `admin` administrator account cannot be restricted to an ADOM. Other administrators are restricted to their ADOM, and cannot configure ADOMs or global settings.

To enable ADOMs

1. Log in with the `admin` account.

Other administrators do not have permissions to configure ADOMs.



Back up your configuration. Enabling ADOMs changes the structure of your configuration, and moves non-global settings to the `root` ADOM. For information on how to back up the configuration, see [“execute backup full-config” on page 510](#).

2. Enter the following commands:

```
config system global
set adom-admin enable
end
```

FortiWeb terminates your administrative session.

3. Log in again.

When ADOMs are enabled, and if you log in as `admin`, the top level of the shell changes: the two top level items are `config global` and `config vdom`.

- `config global` contains settings that only `admin` or other accounts with the `prof_admin` access profile can change.
- `config vdom` contains each ADOM and its respective settings.

This menu and CLI structure change is not visible to non-global accounts; ADOM administrators' navigation menus continue to appear similar to when ADOMs are disabled, except that global settings such as network interfaces, HA, and other global settings do not appear.

4. Continue by defining ADOMs ([“Defining ADOMs”](#)).

To disable ADOMs

1. Delete all ADOM administrator accounts.



Back up your configuration. Disabling ADOMs changes the structure of your configuration, and deletes most ADOM-related settings. It keeps settings from the `root` ADOM only. For information on how to back up the configuration, see [“execute backup full-config” on page 510](#).

2. Enter the following commands:

```
config system global
set adom-admin disable
end
```

FortiWeb terminates your administrative session.

3. Continue by reconfiguring the appliance (see the [FortiWeb Administration Guide](#)).

See also

- [Permissions](#)
- [Defining ADOMs](#)
- [Assigning administrators to an ADOM](#)
- `config system admin`
- `config system accprofile`

Defining ADOMs

Some settings can only be configured by the `admin` account — they are **global**. Global settings apply to the appliance overall regardless of ADOM, such as:

- operation mode
- network interfaces
- system time
- backups
- administrator accounts
- access profiles
- FortiGuard connectivity settings
- HA and configuration sync
- SNMP
- RAID
- X.509 certificates
- TCP `SYN` flood anti-DoS setting
- vulnerability scans
- `exec ping` and other global operations that exist only in the CLI

Only the `admin` account can configure global settings.



In the current release, some settings, such as user accounts for HTTP authentication, anti-defacement, and logging destinations are read-only for ADOM administrators. Future releases will allow ADOM administrators to configure these settings separately for their ADOM.

Other settings can be configured separately for each ADOM. They essentially define each ADOM. For example, the policies of `adom-A` are separate from `adom-B`.

Initially, only the `root` ADOM exists, and it contains settings such as policies that were global before ADOMs were enabled. Typically, you will create additional ADOMs, and few if any administrators will be assigned to the `root` ADOM. After ADOMs are created, the `admin` account usually assigns other administrator accounts to configure their ADOM-specific settings. However, as the `root` account, the `admin` administrator does have permission to configure all settings, including those within ADOMs.

To create an ADOM

1. Log in with the `admin` account.

Other administrators do not have permissions to configure ADOMs.

2. Enter the following commands:

```
config vdom
edit <adom_name>
```

where <adom_name> is the name of your new ADOM. (Alternatively, to configure the default root ADOM, type `root`.)



The maximum number of ADOMs you can add varies by your FortiWeb model. The number of ADOMs is limited by available physical memory (RAM), and therefore also limits the maximum number of policies and sessions per ADOM. See the [FortiWeb Administration Guide](#).

The new ADOM exists, but its settings are not yet configured.

3. Either:

- assign another administrator account to configure the ADOM (continue with “[Assigning administrators to an ADOM](#)”), or
- configure the ADOM yourself by entering commands such as:

```
config log...
config server-policy...
config system...
config waf...
```

See also

- [Assigning administrators to an ADOM](#)
- [Administrative domains \(ADOMs\)](#)
- [Permissions](#)
- [config system admin](#)
- [config system accprofile](#)

Assigning administrators to an ADOM

The `admin` administrator can create other administrators and assign their account to an ADOM, constraining them to that ADOM’s configurations and data.

To assign an administrator to an ADOM

1. If you have not yet created any administrator access profiles, create at least one. See “[config system accprofile](#)” on page 167.
2. In the administrator account’s `accprofile <access-profile_name>` setting, select the new access profile.
(Administrators assigned to the `prof_admin` access profile will have global access. They cannot be restricted to an ADOM.)
3. In the administrator account’s `domains <adom_name>` setting, select the account’s assigned ADOM. Currently, in this version of FortiWeb, administrators cannot be assigned to more than one ADOM.

See also

- [Permissions](#)
- [config system admin](#)
- [config system accprofile](#)
- [Defining ADOMs](#)

config

The `config` commands configure your FortiWeb appliance's feature settings.

This chapter describes the following commands:

<code>config log alertemail</code>	<code>config server-policy pattern data-type-group</code>	<code>config system conf-sync</code>
<code>config log attack-log</code>	<code>config server-policy pattern suspicious-url-rule</code>	<code>config system dns</code>
<code>config log custom-sensitive-rule</code>	<code>config server-policy policy</code>	<code>config system dos-prevention</code>
<code>config log disk</code>	<code>config server-policy pserver</code>	<code>config system fail-open</code>
<code>config log email-policy</code>	<code>config server-policy pservers</code>	<code>config system global</code>
<code>config log event-log</code>	<code>config server-policy service custom</code>	<code>config system ha</code>
<code>config log forti-analyzer</code>	<code>config server-policy service predefined</code>	<code>config system interface</code>
<code>config log fortianalyzer-policy</code>	<code>config server-policy vserver</code>	<code>config system ip-detection</code>
<code>config log memory</code>	<code>config system accprofile</code>	<code>config system network-option</code>
<code>config log reports</code>	<code>config system admin</code>	<code>config system raid</code>
<code>config log sensitive</code>	<code>config system advanced</code>	<code>config system settings</code>
<code>config log syslogd</code>	<code>config system antivirus</code>	<code>config system snmp community</code>
<code>config log syslog-policy</code>	<code>config system autoupdate override</code>	<code>config system snmp sysinfo</code>
<code>config log traffic-log</code>	<code>config system autoupdate schedule</code>	<code>config system v-zone</code>
<code>config log trigger-policy</code>	<code>config system autoupdate tunneling</code>	<code>config user admin-usergrp</code>
<code>config router setting</code>	<code>config system backup</code>	<code>config user ldap-user</code>
<code>config router static</code>	<code>config system certificate ca</code>	<code>config user local-user</code>
<code>config server-policy allow-hosts</code>	<code>config system certificate ca-group</code>	<code>config user ntlm-user</code>
<code>config server-policy custom-application application-policy</code>	<code>config system certificate crl</code>	<code>config user radius-user</code>
<code>config server-policy custom-application url-replacer</code>	<code>config system certificate intermediate-certificate</code>	<code>config user user-group</code>
<code>config server-policy dserver</code>	<code>config system certificate intermediate-certificate-group</code>	<code>config wad website</code>
<code>config server-policy error-page</code>	<code>config system certificate local</code>	<code>config waf allow-method-exceptions</code>
<code>config server-policy health</code>	<code>config system certificate remote</code>	<code>config waf allow-method-policy</code>
<code>config server-policy http-content-routing-policy</code>	<code>config system console</code>	<code>config waf application-layer-dos-prevention</code>
<code>config server-policy pattern custom-data-type</code>	<code>config system certificate verify</code>	<code>config waf base-signature-disable</code>
<code>config server-policy pattern custom-global-white-list-group</code>		<code>config waf brute-force-login</code>
<code>config server-policy pattern custom-susp-url</code>		<code>config waf custom-access policy</code>
<code>config server-policy pattern custom-susp-url-rule</code>		<code>config waf custom-access rule</code>

config waf custom-protection-group	config waf http-request-flood-prevention-rule	config waf url-access url-access-policy
config waf custom-protection-rule	config waf input-rule	config waf url-access url-access-rule
config waf exclude-url	config waf ip-intelligence	config waf url-rewrite url-rewrite-policy
config waf file-compress-rule	config waf ip-intelligence-exception	config waf url-rewrite url-rewrite-rule
config waf file-uncompress-rule	config waf ip-list	config waf web-cache-exception
config waf file-upload-restriction-policy	config waf layer4-access-limit-rule	config waf web-cache-policy
config waf file-upload-restriction-rule	config waf layer4-connection-flood-check-rule	config waf web-protection-profile autolearning-profile
config waf geo-block-list	config waf padding-oracle	config waf web-protection-profile inline-protection
config waf hidden-fields-protection	config waf page-access-rule	config waf web-protection-profile offline-protection
config waf hidden-fields-rule	config waf parameter-validation-rule	config waf x-forwarded-for
config waf http-authen http-authen-policy	config waf signature	config wvs policy
config waf http-authen http-authen-rule	config waf site-publish-helper policy	config wvs profile
config waf http-connection-flood-check-rule	config waf site-publish-helper rule	config wvs schedule
config waf http-constraints-exceptions	config waf start-pages	
config waf http-protocol-parameter-restriction		



Although not usually explicitly shown in each config command's "Syntax" section, for all `config` commands, there are related `get` and `show` commands which display that part of the configuration, either in the form of a list of settings and values, or commands that are required to achieve that configuration from the firmware's default state, respectively. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned.

log alertemail

Use this command to enable or disable alert emails, and to choose which email policy to use with them. Alert emails notify administrators or other personnel when an alert condition occurs, such as a system failure or network attack.

The email address information and the alert message intervals are configured separately for each email policy. For information on the severity levels of log messages associated with an email policy, see [“config log email-policy” on page 72](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log alertemail
    set status {enable | disable}
    set email-policy <policy_name>
end
```

Variable	Description	Default
status {enable disable}	Enable to generate an alert email when the FortiWeb appliance records a log message, if that log message meets or exceeds the severity level configured in “config log email-policy” on page 72 .	enable
email-policy <policy_name>	Type the name of a previously configured email policy. The maximum length is 35 characters. To display a list of the existing email policies, type: set email-policy ?	No default.

Example

This example enables alert email when either a system event or attack log message is logged. The alert email is sent using the recipients configured in `emailpolicy1`.

```
config log alertemail
    set status enable
    set email-policy emailpolicy1
end
```

Related topics

- [config log email-policy](#)

log attack-log

Use this command to configure recording of attack log messages on the local FortiWeb disk.



You must enable disk log storage and select log severity levels using the [config log disk](#) command before any attack logs can be stored on disk.

Also use this command to define specific packet payloads to retain when storing attack logs.

Packet payloads can be retained for specific attack types or validation failures detected by the FortiWeb appliance. Packet payloads supplement the log message by providing the actual data that triggered the attack log, which may help you to fine-tune your regular expressions to prevent false positives. You can also examine changes to attack behavior for subsequent forensic analysis. (Alternatively, for more extensive packet logging, you can run a packet trace. See [“network sniffer” on page 487](#).)

If the offending HTTP request exceeds 4 kilobytes (KB), the FortiWeb appliance retains only 4 KB of the part of the payload that triggered the log message.

You can view attack log packet payloads from the *Packet Log* column using the web UI. For details, see the [FortiWeb Administration Guide](#).

Packet payloads can contain sensitive information. You can prevent sensitive data from display in the packet payload by applying sensitivity rules that detect and obscure sensitive information. For details, see [“config log sensitive” on page 92](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log attack-log
    set status {enable | disable}
    set http-parse-error-output {enable | disable}
    set packet-log {allow-robot | anti-virus-detection | cookie-poison |
    custom-access | custom-protection-rule | hidden-fields-failed |
    http-protocol-constraints | illegal-file-type | illegal-xml-format |
    ip-intelligence | padding-oracle | parameter-rule-failed |
    signature-detection}
end
```

Variable	Description	Default
status {enable disable}	Enable to record attack log messages on the disk. To record attack logs, disk log storage must be enabled, and the severity levels selected using the config log disk command.	enable

Variable	Description	Default
<code>http-parse-error-output</code> {enable disable}	Enable while debugging only, to log errors of the HTTP protocol parser.	disable
<code>packet-log</code> {allow-robot anti-virus-detection cookie-poison custom-access custom-protection-rule hidden-fields-failed http-protocol-constraints illegal-file-type illegal-xml-format ip-intelligence padding-oracle parameter-rule-failed signature-detection}	<p>Select one or more detected attack types or validation failures. FortiWeb will keep packet payloads from its HTTP parser buffer with their associated attack log message.</p> <p>Separate each attack type with a space. To add or remove a packet payload type, re-type the entire space-delimited list with the new option included or omitted.</p> <p>Some options have historical names. Correlations with current feature names are:</p> <ul style="list-style-type: none"> • <code>allow-robot</code> — Known search engines • <code>custom-protection-rule</code> — Custom signature detection (not predefined) <p>To empty this list and keep no packet payloads, effectively disabling the feature, type <code>unset packet-log</code>.</p>	No default.

Example

This example enables log storage on the hard disk and sets `information` as the minimum severity level that a log message must meet in order for the log to be stored. It also enables retention of packet payloads that triggered allowed robots and custom protection rules along with their correlating attack logs. (Conversely, it disables any other packet payload retention that may have been enabled before, because it completely replaces the list each time it is configured.)

```
config log disk
    set status enable
    set severity information
end
config log attack-log
    set status enable
    set packet-log allow-robot custom-protection-rule
end
```

Related topics

- [config log sensitive](#)
- [config log custom-sensitive-rule](#)
- [config log event-log](#)
- [config log traffic-log](#)
- [diagnose debug application miglogd](#)
- [diagnose log](#)

log custom-sensitive-rule

Use this command to configure custom rules to obscure sensitive information that is not obscured in log message packet payloads by the predefined sensitivity rules.

Use this command in conjunction with [“config log sensitive” on page 92](#).

If enabled to do so, a FortiWeb appliance will obscure predefined data types, including user names and passwords in log message packet payloads. If other sensitive data in the packet payload is not obscured by the predefined data types, you can create your own data type sensitivity rules, such as ages or other identifying numbers.



Sensitive data definitions are **not** retroactive. They will hide strings in subsequent log messages, but will not affect existing log messages.

This command is relevant only if you have enabled the FortiWeb appliance to keep packet payloads along with their associated log messages, and have selected to obscure logs according to custom data types. For details, see [“config log attack-log” on page 65](#) and [“config log sensitive” on page 92](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log custom-sensitive-rule
  edit <custom-sensitive-rule_name>
    set expression "<sensitive-type_pattern>"
    set field-name "<parameter-name_pattern>"
    set field-value "<parameter-value_pattern>"
    set type {field-mask-rule | general-mask-rule}
  next
end
```

Variable	Description	Default
<custom-sensitive-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
expression "<sensitive-type_pattern>"	Type a regular expression that matches all and only the strings or numbers that you want to obscure in the packet payloads. For example, to hide a parameter that contains the age of users under 13, you could enter: age\[1-13] Expressions must not start with an asterisk (*). The maximum length is 255 characters.	No default.

Variable	Description	Default
type {field-mask-rule general-mask-rule}	<p>Select either <code>general-mask-rule</code> (a regular expression that will match any substring in the packet payload) or <code>field-mask-rule</code> (a regular expression that will match only the value of a specific form input).</p> <p>If you select <code>general-mask-rule</code>, configure <code>expression "<sensitive-type_pattern>".</code></p> <p>If you select <code>field-mask-rule</code>, configure <code>field-name "<parameter-name_pattern>"</code> and <code>field-value "<parameter-value_pattern>".</code></p>	general-mask-rule
field-name "<parameter-name_pattern>"	Type a regular expression that matches all and only the input names whose values you want to obscure. (The input name itself will not be obscured. If you wish to do this, use <code>general-mask-rule</code> instead.) The maximum length is 255 characters.	No default.
field-value "<parameter-value_pattern>"	<p>Type a regular expression that matches all and only the input values that you want to obscure. The maximum length is 255 characters.</p> <p>For example, to hide a parameter that contains the age of users under 13, for <code>field-name "<parameter-name_pattern>"</code>, you would enter <code>age</code>, and for <code>field-value "<parameter-value_pattern>"</code>, you could enter <code>[1-13]</code>.</p> <p>Valid expressions must not start with an asterisk (*).</p> <p>Caution: Field masks using asterisks are greedy: a match for the parameter's value will obscure it, but will also obscure the rest of the parameters in the line. To avoid this, enter an expression whose match terminates with, but does not consume, the parameter separator.</p> <p>For example, if parameters are separated with an ampersand (&), and you want to obscure the value of the field name <code>username</code> but not any of the parameters that follow it, you could enter the field value:</p> <p><code>. *? (? = \&)</code></p> <p>This would result in:</p> <p><code>username****&age=13&origurl=%2Flogin</code></p>	No default.

Example

This example enables the FortiWeb appliance to keep all types of packet payloads with their associated log messages. It also enables and defines a custom sensitive data type (applies to age 13 or less) that will be obscured in logs.

```
config log attack-log
    set status enable
    set packet-log allow-robot anti-virus-detection cookie-poison
    custom-access custom-protection-rule hidden-fields-failed http-
    protocol-constraints illegal-file-type illegal-xml-format ip-
```

```
        intelligence padding-oracle parameter-rule-failed signature-  
        detection  
    end  
    config log sensitive  
        set type custom-rule  
    end  
    config log custom-sensitive-rule  
        edit rule1  
            set type general-mask-rule  
            set expression "age\\=[1-13]*$"  
        next  
    end
```

Related topics

- [config log sensitive](#)
- [config log attack-log](#)
- [config log traffic-log](#)

log disk

Use this command to enable and configure recording of log messages to the local hard disk.



Logging must be enabled for each individual log type before log messages will be recorded to disk. See [config log attack-log](#), [config log event-log](#), and [config log traffic-log](#) for details.

You can use SNMP traps to notify you when disk space usage exceeds 80%. For details, see “[config system snmp community](#)” on page 234.

You can generate reports based upon log messages that you save to the local hard disk. For details, see “[config log reports](#)” on page 83.

Syntax

```
config log disk
  set diskfull {nolog | overwrite}
  set max-log-file-size <file-size_int>
  set severity {alert | critical | debug | emergency | error |
  information | notification | warning}
  set status {enable | disable}
end
```

Variable	Description	Default
status {enable disable}	Enable to store log messages on the local hard disk. Log messages are stored only if logging is enabled for the individual log types using the config log attack-log , config log event-log , and config log traffic-log commands. Also configure severity, diskfull and max-log-file-size.	enable
diskfull {nolog overwrite}	Type what the FortiWeb appliance will do when the local disk is full and a new log message is caused, either: <ul style="list-style-type: none">nolog — Discard the new log message.overwrite — Delete the oldest log file in order to free disk space, then store the new log message. This field is available only if status is enable.	overwrite

Variable	Description	Default
max-log-file-size <file-size_int>	Type the maximum size in megabytes (MB) of the current log file. When the log file reaches the maximum size the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started). The valid range is between 100 and 200 MB. This field is available only if <code>status</code> is <code>enable</code> .	100
severity {alert critical debug emergency error information notification warning}	Select the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to record it.	information

Example

This example enables logging of event and attack logs and recording of the log messages to the local hard disk. Only the log messages with a severity of `notification` or higher are recorded. If all free space on the hard disk is consumed and a new log message is generated, the `diskfull` option determines that the FortiWeb will overwrite the oldest log message. The log messages are saved to a separated log file for each message type. Once the log file size reaches the 100 MB specified by `max-log-file-size`, the FortiWeb appliance saves the log file with a sequentially-numbered name and starts a new log.

```
config log event-log
    set status enable
end
config log attack-log
    set status enable
end
config log disk
    set status enable
    set severity notification
    set diskfull overwrite
    set max-log-file-size 100
end
```

Related topics

- [config log attack-log](#)
- [config log event-log](#)
- [config log traffic-log](#)
- [config system snmp community](#)
- [config log reports](#)
- [execute formatlogdisk](#)

log email-policy

Use this command to create an email policy. An email policy identifies email recipients, email address, email connection requirements and authentication information, if required.

You can configure multiple email policies and apply those policies as required in different situations. The FortiWeb appliance can be configured to send email for different situations, such as to alert administrators when certain system events or rule violations occur, or when log reports are available for distribution.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log email-policy
edit <email-policy_name>
    set mailfrom <address_str>
    set mailto1 <recipient_email>
    set mailto2 <recipient_email>
    set mailto3 <recipient_email>
    set smtp-server {<smtp_ipv4> | <smtpfqdn>}
    set smtp-auth {enable | disable}
    set smtp-username <auth_str>
    set smtp-password <password_str>
    set severity {alert | critical | debug | emergency | error |
information | notification | warning}
    set alert-interval <minutes_int>
    set critical-interval <minutes_int>
    set debug-interval <minutes_int>
    set emergency-interval <minutes_int>
    set error-interval <minutes_int>
    set information-interval <minutes_int>
    set notification-interval <minutes_int>
    set warning-interval <minutes_int>
next
end
```

Variable	Description	Default
<email-policy_name>	Type the name of an email policy. The maximum length is 35 characters.	No default.
mailfrom <address_str>	Type the sender email address, such as FortiWeb@example.com, that the FortiWeb appliance will use when sending email. The maximum length is 63 characters.	No default.
mailto1 <recipient_email>	Type the email address of the first recipient, such as admin@example.com, to which the FortiWeb appliance will send email. You must enter one email address for alert email to function. The maximum length is 63 characters.	No default.

Variable	Description	Default
mailto2 <recipient_email>	Type the email address of the second recipient, if any, to which the FortiWeb appliance will send alert email. The maximum length is 63 characters.	No default.
mailto3 <recipient_email>	Type the email address of the third recipient, if any, to which the FortiWeb appliance will send alert email. The maximum length is 63 characters.	No default.
smtp-server {<smtp_ipv4> <smtpfqdn>}	Type the IP address or fully qualified domain name (FQDN) of the SMTP server, such as mail.example.com, that the FortiWeb appliance can use to send email. The maximum length is 63 characters.	No default.
smtp-auth {enable disable}	Enable if the SMTP server requires authentication. Also enable if authentication is not required but is available and you want the FortiWeb appliance to authenticate.	disable
smtp-username <auth_str>	If you enable smtp-auth {enable disable} , type the user name that the FortiWeb appliance will use to authenticate itself with the SMTP relay. The maximum length is 63 characters. This field is available only if you enable smtp-auth {enable disable} .	No default.
smtp-password <password_str>	If you enable smtp-auth {enable disable} , type the password that corresponds with the user name. This field is available only if you enable smtp-auth {enable disable} .	No default.
severity {alert critical debug emergency error information notification warning}	Select the severity threshold that log messages must meet or exceed in order to cause an email alert.	emergency
emergency-interval <minutes_int>	Type the interval in minutes between each email message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is emergency continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	1
alert-interval <minutes_int>	Type the interval in minutes between each email message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is alert continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	2

Variable	Description	Default
critical-interval <minutes_int>	Type the interval in minutes between each email message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is critical continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	3
error-interval <minutes_int>	Type the interval in minutes between each email message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is error continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	5
notification-interval <minutes_int>	Type the interval in minutes between each message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is notification continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	20
warning-interval <minutes_int>	Type the interval in minutes between each email message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is warning continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	10
information-interval <minutes_int>	Type the interval in minutes between each email message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is information continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	30
debug-interval <minutes_int>	Type the interval in minutes between each email message that the FortiWeb appliance will send after the initial email, as long as events whose severity level is debug continue to occur, triggering additional email. The valid range is from 1 to 2,147,483,647 minutes.	60

Example

This example creates email policy for use in multiple situations. When the email policy is attached to rule violations or log reports, an email will be sent from `fortiweb@example.com`, to `admin@example.com` and `analysis@example.com`, using an SMTP server `mail.example.com`. The SMTP server requires authentication. The FortiWeb appliance will authenticate as `fortiweb` when connecting to the SMTP server.

Log messages more severe than a notification are logged. As long as events continue to trigger notification-level log messages, the FortiWeb appliance will send an alert email every 10 minutes. (Log messages of other severity levels will trigger alert email at their default intervals.)

When the configuration is complete, the administrator should log in to the web UI to send a sample alert email to test the configuration and the email system, verifying the complete path between the FortiWeb appliance and the inbox for the email account `admin@example.com`.

```
config log email-policy
  edit Email_Policy1
    set mailfrom fortiweb@example.com
    set mailto1 admin@example.com
    set mailto2 analysis@example.com
    set smtp-server mail.example.com
    set smtp-auth enable
    set smtp-username fortiweb
    set smtp-password fortiWebPassworD2
    set severity notification
    set notification-interval 10
  next
end
```

Related topics

- [config log alertemail](#)
- [config log trigger-policy](#)
- [config system dns](#)
- [config router static](#)

log event-log

Use this command to configure recording of event log messages, and then use other commands to store those messages on the local FortiWeb disk, in local FortiWeb memory, or both. Use other commands to configure a traffic log and attack log.



You must enable disk and/or memory log storage and select log severity levels before FortiWeb will store any event logs.

Syntax

```
config log event-log
    set status {enable | disable}
    set threshold {50 | 60 | 70 | 80 | 90}
    set cpu-high <percentage_int>
    set mem-high <percentage_int>
    set trigger-policy <trigger-policy_name>
end
```

Variable	Description	Default
status {enable disable}	Enable to record event log messages. To select the destination and the severity threshold of the stored log messages, used either the config log disk or the config log memory command.	enable
threshold {50 60 70 80 90}	Select a threshold level as a percentage that will trigger an event log when the actual number of persistent server sessions reaches the defined percentage of the total number of persistent server sessions allowed for the FortiWeb appliance.	50
cpu-high <percentage_int>	Type a threshold level as a percentage beyond which CPU usage will trigger an event log entry. The valid range is from 60 to 99 percent.	60
mem-high <percentage_int>	Type a threshold level as a percentage beyond which memory usage will trigger an event log entry. The valid range is from 60 to 99 percent.	60
trigger-policy <trigger-policy_name>	Type the name of the trigger to apply when the CPU, memory, or number of sessions meets or exceeds the threshold (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.

Example

This example enables recording of event logs, enables disk log storage and memory log storage, and sets `alert` as the minimum severity level that a log message must achieve for storage.

```
config log disk
    set status enable
    set severity alert
end
config log memory
    set status enable
    set severity alert
end
config log event-log
    set status enable
end
```

Related topics

- [config log disk](#)
- [config log memory](#)
- [config log attack-log](#)
- [config log traffic-log](#)
- [diagnose debug application miglogd](#)
- [diagnose log](#)

log forti-analyzer

Use this command to configure the FortiWeb appliance to send its log messages to a remote FortiAnalyzer appliance.

You must first define one or more FortiAnalyzer policies using [config log fortianalyzer-policy](#).

Logs sent to FortiAnalyzer are controlled by FortiAnalyzer policies and trigger actions that you configure on the FortiWeb appliance, and are associated with various types of violations.



Usually, you should set trigger actions for specific types of violations. Failure to do so will result in the FortiWeb appliance logging every occurrence, which could result in high log volume and reduced system performance. Excessive logging for an extended period of time may cause premature hard disk failure.



Logs stored remotely cannot be viewed from the web UI, and cannot be used by FortiWeb to build reports. If you require these features, record logs locally as well as remotely.

Syntax

```
config log forti-analyzer
  set fortianalyzer-policy <policy_name>
  set severity {alert | critical | debug | emergency | error |
  information | notification | warning}
  set status {enable | disable}
end
```

Variable	Description	Default
fortianalyzer-policy <policy_name>	Type the name of an existing FortiAnalyzer policy to use when storing log information remotely. The maximum length is 35 characters. To view a list of the existing FortiAnalyzer policies, type: set fortianalyzer-policy ?	No default.
status {enable disable}	Enable to record event log messages in memory if it meets or exceeds the severity level configured in severity.	disable
severity {alert critical debug emergency error information notification warning}	Select the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to save it to memory.	information

Example

This example enables FortiAnalyzer logging and recording of the log messages. Only the log messages with a severity of `error` or higher are recorded.

```
config log forti-analyzer
  set status enable
  set severity error
end
```

Related topics

- [config log fortianalyzer-policy](#)

log fortianalyzer-policy

Use this command to create policies for use by protection rules to store log messages remotely on a FortiAnalyzer appliance. For example, once you create a FortiAnalyzer policy, you can include it in a trigger policy, which in turn can be applied to a trigger action in a protection rule.

You need to create a FortiAnalyzer policy if you also plan to send log messages to a FortiAnalyzer appliance.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log fortianalyzer-policy
  edit <policy_name>
    set ip-address <forti-analyzer_ipv4>
  next
end
```

Variable	Description	Default
<policy_name>	Type the name of the new or existing FortiAnalyzer policy. The maximum length is 35 characters. To display a list of the existing policies, type: edit ?	No default.
ip-address <forti-analyzer_ipv4>	Type the IP address of the remote FortiAnalyzer appliance.	No default.

Example

This example creates a policy entry and assigns an IP address, then enables FortiAnalyzer logging for log messages with a severity of `error` or higher

```
config log fortianalyzer-policy
  edit fa-policy1
    set ip-address 192.0.2.0
  next
end
config log forti-analyzer
  set fortianalyzer-policy fa-policy1
  set status enable
  set severity error
end
```

Related topics

- [config log forti-analyzer](#)

log memory

Use this command to enable and configure event logging to memory (RAM). Only event logs can be stored in local memory.



Do **not** store important log messages to memory only. Memory is not permanent storage. Log messages stored in memory will be lost upon reboot or shutdown.



Event message logging must be enabled before event messages are recorded to memory. See [config log event-log](#) for details.



For improved performance, when not necessary, avoid logging highly frequent log types. Logs stored in memory consume RAM that could otherwise be used for scanning and other features, affecting FortiWeb's throughput speed.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config log memory
    set severity {alert | critical | debug | emergency | error |
    information | notification | warning}
    set status {enable | disable}
end
```

Variable	Description	Default
status {enable disable}	Enable to record event log messages in memory if they meet or exceed the severity level configured in <code>severity</code> .	enable
severity {alert critical debug emergency error information notification warning}	Type the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to save it to memory.	information

Example

This example enables event logging and recording of the log messages at the `error` level to memory.

```
config log event-log
    set status enable
end
config log memory
    set status enable
    set severity error
end
```

Related topics

- [config log event-log](#)

log reports

Use this command to configure report profiles.

When generating a report, FortiWeb appliances collate information collected from their log files and present the information in tabular and graphical format.

In addition to log files, your FortiWeb appliance requires a report profile to generate a report. A report profile is a group of settings that contains the report name, file format, subject matter, and other aspects that the FortiWeb appliance considers when generating the report.

FortiWeb appliances can generate reports automatically, according to the schedule that you configure in the report profile, or manually in the web UI when you click the *Run now* icon in the report profile list. You may want to create one report profile for each type of report that you will generate on demand or periodically, by schedule.



Generating reports can be resource intensive. To avoid email processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night.

The number of results in a section's table or graph varies by the report type.

Ranked reports (top *x*, or top *y* of top *x*) can include a different number of results per cross-section, then combine remaining results under "Others." For example, in "Top Attack Severity by Hour of Day," the report includes the top *x* hours, and their top *y* attacks, then groups the remaining results.

- `scope_top1 <topX_int>` is *x*.
- `scope_top2 <topY_int>` is *y*.

Before you generate a report, collect log data that will be the basis of the report. For information on enabling logging to the local hard disk, see ["config log attack-log" on page 65](#) and ["config log disk" on page 70](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see ["Permissions" on page 47](#).



Creating a report profile is considerably easier in the web UI. Go to *Log&Report > Report Config*.

Syntax

```
config log reports
edit <report_name>
    set custom_company "<org_str>"
    set custom_footer_options {custom | report-title}
    set custom_footer "<footer_str>"
    set custom_header <header_str>
    set custom_header_logo <filename_hex>
    set custom_title_logo <filename_hex>
    set email_attachment_compress {enable | disable}
```

```

set email_attachment_name "<filename_str>"
set email_body "<message_str>"
set email_subject "<subject_str>"
set filter_string "<log-filter_str>"
set include_nodata {yes | no}
set on_demand {enable | disable}
set output_email {html mht pdf rtf txt}
set output_email_policy <policy_name>
set output_file {html mht pdf rtf txt}
set period_end <time_str> <date_str>
set period_last_n <n_int>
set period_start <time_str> <date_str>
set period_type {last-14-days | last-2-weeks | last-30-days |
last-7-days | lastmonth | last-n-days | last-n-hours | last-n-
weeks | last-quarter | last-week | other | this-month |
this-quarter | this-week | this-year | today | yesterday}
set report_desc "<comment_str>"
set report_title <title_str>
set Report_attack_activity {attacks-type attacks-url
attacks-date-type attacks-month-type attacks-day-type
attacks-hour-type attacks-type-dev attacks-dst-type attacks-dst-ip
attacks-type-ip attacks-method-type attacks-cat attacks-policy
attacks-day attacks-ts attacks-td attacks-proto
attacks-date-severity attacks-month-severity attacks-day-severity
attacks-hour-severity attacks-sessionid attacks-signature-id
attacks-srccountry attacks-type-signature-id}
set Report_event_activity {ev-all ev-all-cat ev-all-type
ev-crit-hour ev-crit-day ev-warn-hour ev-warn-day ev-info-hour
ev-info-day ev-emer-hour ev-emer-day ev-aler-hour ev-aler-day
ev-err-hour ev-err-day ev-noti-hour ev-noti-day ev-hour
ev-hour-cat ev-day ev-day-cat ev-stat}
set Report_traffic_activity {net-pol net-srv net-src net-dst
net-src-dst net-dst-src net-date-dst net-hour-dst net-day-dst
net-month-dst net-date-src net-hour-src net-day-src net-month-src
net-srccountry}
set Report_pci_activity {pci-attacks-date-type pci-attacks-day-
type pci-attacks-hour-type pci-attacks-month-type}
set schedule_type {daily | dates | days | none}
set schedule_days {sun | mon | tue | wed | thu | fri | sat}
set schedule_dates <dates_str>
set schedule_time <time_str>
set scope_include_summary {yes | no}
set scope_include_table_of_content {yes | no}
set scope_top1 <topX_int>

```

```

set scope_top2 <topY_int>
next
end

```

Variable	Description	Default
<report_name>	Type the name of a new or existing report profile. The maximum length is 63 characters. The profile name will be included in the report header. To display the list of existing report names, type: edit ?	No default.
custom_company "<org_str>"	Type the name of your department, company, or other organization, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 191 characters. For information on enabling the summary, see scope_include_summary {yes no} .	No default.
custom_footer_options {custom report-title}	Select either: <ul style="list-style-type: none">report-title — Use <report_name> as the footer text.custom — Provide separate footer text in custom_footer "<footer_str>".	report-title
custom_footer "<footer_str>"	Type the text, if any, that you want to include at the bottom of each report page. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 127 characters. This setting is available only if custom_footer_options is custom.	No default.
custom_header <header_str>	Type the text, if any, that you want to include at the top of each report page. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 127 characters.	No default.
custom_header_logo <filename_hex>	Type the file name of a custom logo that you have previously uploaded to the FortiWeb appliance. The logo image will be included in the report header. The maximum length is 255 characters.	No default.
custom_title_logo <filename_hex>	Type the file name of a custom logo that you have previously uploaded to the FortiWeb appliance. The logo image will be included in the report title. The maximum length is 255 characters.	No default.
email_attachment_compress {enable disable}	Enable to enclose the generated report formats in a compressed archive attached to the email. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt} .	disable

Variable	Description	Default
email_attachment_name "<filename_str>"	Type the file name that will be used for the reports attached to the email. The maximum length is 63 characters. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt} .	No default.
email_body "<message_str>"	Type the message body of the email. The maximum length is 383 characters. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt} .	No default.
email_subject "<subject_str>"	Type the subject line of the email. The maximum length is 191 characters. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt} .	No default.
filter_string "<log-filter_str>"	Type a log message filter string that includes or excludes log messages based upon matching log field values. The maximum length is 1,023 characters. For example syntax, see “Example” on page 90 .	No default.
include_nodata {yes no}	Select whether to include (yes) or hide (no) reports which are empty because there is no matching log data.	no
on_demand {enable disable}	Enable to run the report one time only. After the FortiWeb appliance completes the report, it removes the report profile from its hard disk. Type <code>disable</code> to schedule a time to run the report, and to keep the report profile for subsequent use.	disable
output_email {html mht pdf rtf txt}	Select one or more file types for the report when mailing generated reports.	No default.
output_email_policy <policy_name>	If you set a value for <code>output_email</code> , type the name of the email policy that contains settings for sending the report by email. The maximum length is 35 characters. For more information on email policies, see “config log email-policy” on page 72 .	No default.
output_file {html mht pdf rtf txt}	Select one or more file types for the report when saving to the FortiWeb hard disk.	html

Variable	Description	Default
period_end <time_str> <date_str>	<p>Enter the time and date that define the end of the span of time whose log messages you want to use when generating the report.</p> <p>The time format is hh:mm and the date format is yyyy/mm/dd, where:</p> <ul style="list-style-type: none"> • hh is the hour according to a 24-hour clock • mm is the minute • yyyy is the year • mm is the month • dd is the day <p>This setting appears only when you select a period_type of other.</p>	No default.
period_last_n <n_int>	<p>Enter the number that defines n if the period_type contains that variable. The valid range is from 1 to 2,147,483,647.</p> <p>This setting appears only when you select a period_type of last-n-days, last-n-hours, or last-n-weeks.</p>	No default.
period_start <time_str> <date_str>	<p>Enter the time and date that defines the beginning of the span of time whose log messages you want to use when generating the report.</p> <p>The time format is hh:mm and the date format is yyyy/mm/dd, where:</p> <ul style="list-style-type: none"> • hh is the hour according to a 24-hour clock • mm is the minute • yyyy is the year • mm is the month • dd is the day <p>This setting appears only when you select a period_type of other.</p>	No default.
period_type {last-14-days last-2-weeks last-30-days last-7-days lastmonth last-n-days last-n-hours last-n-weeks last-quarter last-week other this-month this-quarter this-week this-year today yesterday}	<p>Select the span of time whose log messages you want to use when generating the report.</p> <p>If you select last-n-days, last-n-hours, or last-n-weeks, you must also define n by entering period_last_n <n_int>.</p> <p>If you select other, you must also define the start and end of the report's time range by entering period_start and period_end.</p> <p>The span of time will be included in the summary, if enabled. For information on enabling the summary, see scope_include_summary {yes no}.</p>	last-7-days

Variable	Description	Default
report_desc "<comment_str>"	Type a description of the report, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, surround it with double quotes ("). The maximum length is 63 characters. For information on enabling the summary, see scope_include_summary {yes no} .	No default.
report_title <title_str>	Type a title, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 127 characters. For information on enabling the summary, see scope_include_summary {yes no} .	No default.
Report_attack_activity {attacks-type attacks-url attacks-date-type attacks-month-type attacks-day-type attacks-hour-type attacks-type-dev attacks-dst-type attacks-dst-ip attacks-type-ip attacks-method-type attacks-cat attacks-policy attacks-day attacks-ts attacks-td attacks-proto attacks-date-severity attacks-month-severity attacks-day-severity attacks-hour-severity attacks-sessionid attacks-signature-id attacks-srccounty attacks-type-signature-id}	Type zero or more options to indicate which charts based upon attack logs to include in the report. For example, to include “Attacks By Policy,” enter a list of charts that includes attacks-policy. To include “Top Attacked HTTP Methods by Type,” enter a list of charts that includes attacks-method-type.	No default.
Report_event_activity {ev-all ev-all-cat ev-all-type ev-crit-hour ev-crit-day ev-warn-hour ev-warn-day ev-info-hour ev-info-day ev-emer-hour ev-emer-day ev-aler-hour ev-aler-day ev-err-hour ev-err-day ev-noti-hour ev-noti-day ev-hour ev-hour-cat ev-day ev-day-cat ev-stat}	Type zero or more options to indicate which charts based upon event logs to include in the report. For example, to include “Top Event Categories by Status”, enter a list of charts that includes ev-status.	No default.

Variable	Description	Default
Report_traffic_activity {net-pol net-srv net-src net-dst net-src-dst net-dst-src net-date-dst net-hour-dst net-day-dst net-month-dst net-date-src net-hour-src net-day-src net-month-src net-srccountry}	Type zero or more options to indicate which charts based upon traffic logs to include in the report. For example, to include “Top Sources By Day of Week”, enter a list of charts that includes net-day-src.	No default.
Report_pci_activity {pci-attacks-date-type pci-attacks-day-type pci-attacks-hour-type pci-attacks-month-type}	Type zero or more options to indicate which charts based upon PCI attack logs to include in the report.	No default.
schedule_type {daily dates days none}	Select when the FortiWeb appliance will automatically run the report. If you reboot the FortiWeb appliance while the report is being generated, report generation resumes after the boot process is complete. If schedule_type is daily, dates or days, specify the schedule_time, schedule_days, or schedule_dates when the report will be generated. If schedule_type is none, the report will be generated only when you manually initiate it.	none
schedule_days {sun mon tue wed thu fri sat}	If schedule_type is days, select the day of the week when the report should be generated.	No default.
schedule_dates <dates_str>	If schedule_type is dates, select the specific date of the month, from 1 to 31, when the report should be generated. Separate multiple dates with spaces.	No default.
schedule_time <time_str>	If schedule_type is not none, select the time of day when the report should be run. The time format is hh:mm, where: <ul style="list-style-type: none"> • hh is the hour according to a 24-hour clock • mm is the minute 	00:00
scope_include_summary {yes no}	Enter yes to include a summary section at the beginning of the report. The summary includes: <ul style="list-style-type: none"> • <report_name> • custom_company "<org_str>" • report_desc "<comment_str>" • the date and time when the report was generated using this profile • the span of time whose log messages were used to generate the report, according to period_type 	yes
scope_include_table_of_content {yes no}	Enter yes to include a table of contents at the beginning of the report. The table of contents includes links to each chart in the report.	yes

Variable	Description	Default
scope_top1 <topX_int>	<p>Enter x number of items (up to 30) to include in the first cross-section of ranked reports.</p> <p>For some report types, you can set the top ranked items for the report. These reports have “Top” in their name, and will always show only the top x entries. Reports that do not include “Top” in their name show all information. Changing the values for top field will not affect these reports.</p>	6
scope_top2 <topY_int>	<p>Enter y number of items (up to 30) to include in the second cross-section of ranked reports.</p> <p>For some report types, you can set the number of ranked items to include in the report. These reports have “Top” in their name, and will always show only the top x entries. Some report types have two levels of ranking: the top y sub-entries for each top x entry.</p> <p>Reports that do not include “Top” in their name show all information. Changing the values for top field will not affect these reports.</p>	3

Example

This example configures a report to be generated every Saturday at 1 PM. The report, whose title is “Report 1”, includes all available charts, and covers the last 14 days’ worth of event, traffic, and attack logs. However, it only uses logs where the source IP address was 172.16.1.20. Each time it is generated, it will be saved to the hard disk in both HTML and PDF file formats and will be sent by email in PDF format to recipients defined within the “Log report analysis” email policy.

```
config log reports
edit "Report_1"
    set Report_attack_activity attacks-type attacks-url attacks-date-
    type attacks-month-type attacks-day-type attacks-hour-type
    attacks-type-dev attacks-dst-type attacks-dst-ip attacks-type-ip
    attacks-method-type attacks-cat attacks-policy attacks-day
    attacks-ts attacks-td attacks-proto attacks-date-severity attacks-
    month-severity attacks-day-severity attacks-hour-severity attacks-
    sessionid attacks-signature-id attacks-srccounty attacks-type-
    signature-id
    set Report_event_activity ev-all ev-all-cat ev-all-type ev-crit-
    hour ev-crit-day ev-warn-hour ev-warn-day ev-info-hour ev-info-day
    ev-emer-hour ev-emer-day ev-aler-hour ev-aler-day ev-err-hour ev-
    err-day ev-noti-hour ev-noti-day ev-hour ev-hour-cat ev-day ev-
    day-cat ev-stat
    set Report_traffic_activity net-pol net-srv net-src net-dst net-
    src-dst net-dst-src net-date-dst net-hour-dst net-day-dst net-
    month-dst net-date-src net-hour-src net-day-src net-month-src
    set custom_company "Example, Inc."
    set custom_footer_options custom
    set custom_header "A fictitious corporation."
    set custom_title_logo "titlelogo.jpg"
    set filter_string "(and src==\'172.16.1.10\')"
    set include_nodata yes
```

```
set output_file html pdf
set output_email html
set output_email_policy log_report_analysis
set period_type last-n-days
set report_desc "A sample report."
set report_title "Report 1"
set schedule_type days
set custom_footer "Weekly report for Example, Inc."
set period_last_n 14
set schedule_days sat
set schedule_time 01:00
next
end
```

Related topics

- [config log attack-log](#)
- [config log disk](#)
- [config log email-policy](#)

log sensitive

Use this command to configure whether the FortiWeb appliance will obscure sensitive information, such as user names and passwords, in log messages for which packet payloads are enabled. Each packet payload has predefined sensitivity rules based on the payload data type. If needed, you can also create custom sensitivity rules to obscure other payload data types using [“config log custom-sensitive-rule” on page 67](#).

This command is relevant only if you have enabled the FortiWeb appliance to keep packet payloads along with their associated log messages. For details, see [“config log attack-log” on page 65](#) and [“config log traffic-log” on page 97](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log sensitive
    set type {custom-rule | pre-defined-rule}
end
```

Variable	Description	Default
type {custom-rule pre-defined-rule}	Select whether the FortiWeb appliance will obscure packet payloads according to predefined data types and/or custom data types. See “config log custom-sensitive-rule” on page 67 .	No default.

Example

This example enables the FortiWeb appliance to use a custom sensitive rule to obscure packet payload information that displays information about users that are age 13 and under.

```
config log sensitive
    set type custom-rule
end
config log custom-sensitive-rule
    edit custom-sensitive-rule1
        set type general-mask-rule
        set expression "age\=[1-13]*$"
    next
end
```

Related topics

- [config log custom-sensitive-rule](#)
- [config log attack-log](#)
- [config log traffic-log](#)

log syslogd

Use this command to configure the FortiWeb appliance to send log messages to a Syslog server defined by the [config log syslog-policy](#) command.



For improved performance, unless necessary, avoid logging highly frequent log types. While logs sent to your Syslog server do not persist in FortiWeb's local RAM, FortiWeb still must use bandwidth and processing resources while sending the log message.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log syslogd
    set status {enable | disable}
    set facility {alert | audit | auth | authpriv | clock | cron |
daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 |
local5 | local6 | local7 | mail | ntp | user}
    set severity {alert | critical | debug | emergency | error |
information | notification | warning}
    set policy <syslogd-policy_name>
end
```

Variable	Description	Default
status {enable disable}	Enable to send log messages to the Syslog server defined by config log syslog-policy . Also configure facility, policy and severity.	disable
facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 mail ntp user}	Type the facility identifier that the FortiWeb appliance will use to identify itself when sending log messages to the first Syslog server. To easily identify log messages from the FortiWeb appliance when they are stored on the Syslog server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.	local7
severity {alert critical debug emergency error information notification warning}	Select the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to send it to the first Syslog server.	information
policy <syslogd-policy_name>	If logging to a Syslog server is enabled, type the name of a Syslog policy which describes the Syslog server to which the log message will be sent. The maximum length is 35 characters. For more information on Syslog policies, see “config log syslog-policy” on page 95 .	No default.

Example

This example enables storage of log messages with the `notification` severity level and higher on the Syslog server. The network connections to the Syslog server are defined in `Syslog_Policy1`. The FortiWeb appliance uses the facility identifier `local7` when sending log messages to the Syslog server to differentiate its own log messages from those of other network devices using the same Syslog server.

```
config log syslogd
    set status enable
    set severity notification
    set facility local7
    set policy Syslog_Policy1
end
```

log syslog-policy

Use this command to configure a connection to a Syslog server. A unique policy is required for each Syslog server. The policy is used by the `log syslogd` configuration to define the specific Syslog server on which log messages are stored. For more information, see [“config log syslogd” on page 93](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log syslog-policy
  edit <policy_name>
    set csv {enable | disable}
    set port <port_int>
    set server <syslog_ipv4>
  end
```

Variable	Description	Default
<policy_name>	Type the name of a new or existing Syslog policy. The maximum length is 35 characters. The name of the report profile will be included in the report header. To display the list of existing policies, type: <code>edit ?</code>	No default.
csv {enable disable}	Enable if the Syslog server requires the FortiWeb appliance to send log messages in comma-separated value (CSV) format, instead of the standard Syslog format.	disable
port <port_int>	Type the port number on which the Syslog server listens. The valid range is from 1 to 65,535.	514
server <syslog_ipv4>	Type the IP address of the Syslog server.	No default.

Example

This example creates `Syslog_Policy1`. The Syslog server is contacted by its IP address, `192.168.1.10`. Communications occur over the standard port number for Syslog, UDP port `514`. The FortiWeb appliance sends log messages to the Syslog server in CSV format.

```
config log syslog-policy
  edit Syslog_Policy1
    set server 192.168.1.10
    set port 514
    set csv enable
  next
end
```

Related topics

- [config log syslogd](#)
- [config system dns](#)
- [config router static](#)

log traffic-log

Use this command to have the FortiWeb appliance record traffic log messages on its local disk. This command also lets you save packet payloads with the traffic logs.



You must enable disk log storage and select log severity levels using the [config log disk](#) command before any traffic logs will be stored on disk.

Packet payloads supplement the log message by providing the actual data associated with the traffic log, which may help you to analyze traffic patterns.

You can view packet payloads in the *Packet Log* column when viewing a traffic logs using the web UI. For details, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config log traffic-log
    set packet-log {enable | disable}
    set disk-log {enable | disable}
    set status {enable | disable}
end
```

Variable	Description	Default
status {enable disable}	Enable to record traffic log messages if disk log storage is enabled, and the logs meet or exceed the severity levels selected using config log disk .	disable
packet-log {enable disable}	Enable to keep packet payloads stored with their associated traffic log message. For information on obscuring sensitive information in packet payloads, see config log sensitive .	disable
disk-log {enable disable}	Enable to record traffic logs to the hard disk. Disable to record traffic logs only in available RAM. Caution: Frequent logging to the hard disk for long periods of time causes can result in premature failure of the hard disk. Enable this option only while necessary, and disable it when you are done.	disable

Example

This example enables disk log storage, sets `information` as the minimum severity level that a log message must achieve for storage, enables recording of traffic logs and retention of all packet payloads along with the traffic logs.

```
config log disk
    set status enable
    set severity information
end
config log traffic-log
    set status enable
    set packet-log enable
    set disk-log enable
end
```

Related topics

- [config log attack-log](#)
- [config log event-log](#)
- [config log disk](#)
- [config log sensitive](#)
- [diagnose debug application miglogd](#)
- [diagnose log](#)

log trigger-policy

Use this command to configure a trigger policy for use in the notification process.

You apply trigger policies to individual conditions that have an associated action and severity, such as attacks and rule violations. A trigger policy has the following components:

- an email policy (contains the details associated with the recipient email account)
- a Syslog policy (contains details required to communicate with the Syslog server)
- a FortiAnalyzer policy (contains the IP address of the remote FortiAnalyzer appliance)

The trigger policy determines whether an email is sent to administrators when a certain condition occurs and whether the log messages associated with the condition are stored on a Syslog server or FortiAnalyzer.

You define the email, Syslog, and FortiAnalyzer policies before you apply the trigger policy to an individual condition. For more information, see [“config log email-policy” on page 72](#), [“config log syslog-policy” on page 95](#), and [“config log fortianalyzer-policy” on page 80](#).

To use this command, your administrator account’s access control profile must have either w or rw permission to the loggrp area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config log trigger-policy
  edit <trigger-policy_name>
    set email-policy <email-policy_name>
    set syslog-policy <syslog-policy_name>
    set analyzer-policy <fortianalyzer-policy_name>
  next
end
```

Variable	Description	Default
<trigger-policy_name>	Type the name of a new or existing trigger policy. The maximum length is 35 characters.	No default.
email-policy <email-policy_name>	Type the name of the email policy to be used with the trigger policy. The maximum length is 35 characters. If the conditions associated with the trigger policy occur, the email policy determines the recipients of the notification email messages associated with the condition. For more information, see “config log email-policy” on page 72 .	No default.

Variable	Description	Default
syslog-policy <syslog-policy_name>	Type the name of the Syslog policy to be used with the trigger policy. The maximum length is 35 characters. If the conditions associated with the trigger policy occur, the Syslog policy determines which Syslog server the messages are sent to. For more information, see “config log syslog-policy” on page 95 .	No default.
analyzer-policy <fortianalyzer-policy_name>	Type the name of an existing FortiAnalyzer policy to be used with the trigger policy. The maximum length is 35 characters. See “config log fortianalyzer-policy” on page 80 .	No default.

Example

This example creates `Trigger_policy1`, which uses `emailpolicy1` to send email notifications about the condition to specific recipients, and `Syslog_Policy1` to submit the log messages to a specific Syslog server.

```
config log trigger-policy
  edit Trigger_policy1
    set syslog-policy Syslog_Policy1
    set email-policy emailpolicy1
  next
end
```

Related topics

- [config log email-policy](#)
- [config log syslog-policy](#)
- [config log fortianalyzer-policy](#)
- [config waf http-protocol-parameter-restriction](#)
- [config waf signature](#)

router setting

Use this command to change how FortiWeb handles non-HTTP/HTTPS traffic (for example, SSH and FTP) when it is operating in reverse proxy mode.

When this setting is disabled (the default) and FortiWeb is operating in reverse proxy mode, the appliance drops any non-HTTP/HTTPS traffic.

When this setting is enabled and FortiWeb is operating in reverse proxy mode, the appliance handles non-HTTP/HTTPS protocols in the following ways:

- Any non-HTTP/HTTPS traffic destined for a virtual server on the appliance is dropped.
- For any non-HTTP/HTTPS traffic destined for another destination (for example, a back-end server), FortiWeb acts as a router and forwards it based in its destination address.

This command has no effect when FortiWeb is operating in transparent modes, which allow and forward non-HTTP/HTTPS packets by default.



Use this setting only if necessary. For security and performance reasons, if you have a FortiGate with an Internet/public address virtual IP (VIP) that forwards traffic to your FortiWeb, and your FortiWeb is on the same subnet as your web servers, do not use this setting. Instead, configure the VIP to forward:

- only HTTP/HTTPS to FortiWeb, which forwards it to your servers
- specific traffic such as SSH or SFTP directly to your servers

This avoids latency related to an extra hop. It also avoids accidentally forwarding unscanned protocols.

Routing is best effort. Not all protocols may be supported, such as Citrix Receiver (formerly ICA).

FortiWeb appliances are designed to provide in-depth protection specifically for the HTTP and HTTPS protocols. Because of this, when in **reverse proxy mode**, by default, FortiWeb **does not forward non-HTTP/HTTPS protocols** to your protected web servers. (That is, IP-based forwarding is disabled. Traffic is only forwarded if picked up and scanned by the HTTP reverse proxy.) This provides a secure default configuration by blocking traffic to services that might have been unintentionally left open and should not be accessible to the general public.

In some cases, however, a web server provides more services, not just HTTP or HTTPS. A typical exception is a server that also allows SFTP and SSH access. In these cases, enable routing to allow FortiWeb to route the non-HTTP/HTTPS traffic to the server using the server's IP address. For HTTP/HTTPS services, direct traffic to the IP address of the FortiWeb virtual server, which forwards requests to the back-end server after inspection.

This command has no equivalent in the web UI.

Use the following commands to retrieve information about current static route values:

```
config router setting
    get route static
end
```

Use the following commands to view the current value of `ip-forward`:

```
config router setting
    get route setting
end
```

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config router setting
    set ip-forward {enable | disable}
    set ip6-forward {enable | disable}
end
```

Variable	Description	Default
ip-forward {enable disable}	Enable to forward non-HTTP/HTTPS traffic if its IPv4 IP address matches a static route.	disable
ip6-forward {enable disable}	Enable to forward non-HTTP/HTTPS traffic if its IPv6 IP address matches a static route.	disable

Example

This example enables forwarding of non-HTTP/HTTPS traffic, based upon whether the IP address matches a route for the web servers' subnet, and regardless of HTTP proxy pickup.

```
config router setting
    set ip-forward enable
end
```

Related topics

- [config router static](#)
- [get router all](#)

router static

Use this command to configure static routes, including the default gateway.

Static routes direct traffic existing the FortiWeb appliance — you can specify through which network interface a packet will leave, and the IP address of a next-hop router that is reachable from that network interface. The router is aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets' ultimate destinations.

A default route is a special type of static route. A default route matches all packets, and defines a gateway router that can receive and route packets if no more specific static route is defined for the packet's destination IP address.

During installation and setup, you should have configured at least one static route, a default route, that points to your gateway. You may configure additional static routes if you have multiple gateway routers, each of which should receive packets destined for a different subset of IP addresses.

For example, if a web server is directly attached to one of the network interfaces, but all other destinations, such as connecting clients, are located on distant networks such as the Internet, you might need to add only one route: a default route for the gateway router through which the FortiWeb appliance connects to the Internet.

The FortiWeb appliance examines the packet's destination IP address and compares it to those of the static routes. If more than one route matches the packet, the FortiWeb appliance will apply the route with the smallest index number. For this reason, you should give more specific routes a smaller index number than the default route.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config router static
  edit <route_index>
    set device <interface_name>
    set dst <destination_ip>
    set gateway <router_ip>
  next
end
```

Variable	Description	Default
<route_index>	Type the index number of the static route. If multiple routes match a packet, the one with the smallest index number is applied. The valid range is from 1 to 4,294,967,295.	No default.
device <interface_name>	Type the name of the network interface device, such as <code>port1</code> , through which traffic subject to this route will be outbound. The maximum length is 35 characters.	No default.

Variable	Description	Default
dst <destination_ip>	Enter the destination IP address and netmask of traffic that will be subject to this route, separated with a space. To indicate all traffic regardless of IP address and netmask (that is, to configure a route to the default gateway), enter 0.0.0.0 0.0.0.0. or ::/0.	0.0.0.0 0.0.0.0
gateway <router_ip>	Enter the IP address of a next-hop router. Caution: The gateway IP address must be in the same subnet as the interface's IP address. If you change the interface's IP address later, the new IP address must also be in the same subnet as the interface's default gateway address. Otherwise, all static routes and the default gateway will be lost.	0.0.0.0

Example

This example configures a default route that forwards all packets to the gateway router 192.168.1.1, through the network interface named port1.

```
config router static
  edit 0
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.1.1
    set device port1
  next
end
```

Related topics

- [config router setting](#)
- [config system interface](#)
- [config log syslog-policy](#)
- [config server-policy policy](#)
- [config system admin](#)
- [config system dns](#)
- [config system global](#)
- [config system snmp community](#)
- [config wad website](#)
- [execute traceroute](#)
- [diagnose network arp](#)
- [diagnose network ip](#)
- [diagnose network route](#)
- [get router all](#)

server-policy allow-hosts

Use this command to configure protected host groups.

A protected host group contains one or more IP addresses and/or fully qualified domain names (FQDNs). Each entry in the protected host group defines a virtual or real web host, according to the `Host :` field in the HTTP header of requests from clients, that you want the FortiWeb appliance to protect.

For example, if your web servers receive requests with HTTP headers such as:

```
GET /index.php HTTP/1.1
Host : www.example.com
```

you might define a protected host group with an entry of `www.example.com` and select it in the policy. This would reject requests that are not for that host.



A protected hosts group is usually **not** the same as a physical server.

Unlike a physical server, which is a single IP at the network layer, a protected host group should contain **all** network IPs, virtual IPs, and domain names that clients use to access the web server at the application (HTTP) layer.

For example, clients often access a web server via a **public** network such as the Internet. Therefore the protected host group contains domain names, public IP addresses, and public virtual IPs on a network edge router or firewall that are routable from that public network. But the physical server is only the IP address that the FortiWeb appliance uses to forward traffic to the server and, therefore, is often a **private** network address (unless the FortiWeb appliance operates in offline protection or either of the transparent modes).

Protected host groups can be used by:

- policies
- input rules
- server protection exceptions
- start page rules
- page access rules
- URL access rules
- allowed method exceptions
- HTTP authentication rules
- hidden fields rules
- many others

Rules can use protected host definitions to apply rules only to requests for a protected host. If you do not specify a protected host group in the rule, the rule will be applied based upon other criteria such as the URL, but regardless of the `Host :` field.

Policies can use protected host definitions to block connections that are not destined for a protected host. If you do not select a protected host group in a policy, connections will be accepted or blocked regardless of the `Host :` field.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy allow-hosts
  edit <protected-hosts_name>
    set default-action {allow | deny}
    config host-list
      edit <protected-host_index>
        set action {allow | deny}
        set host {<host_ipv4> | <host_fqdn> | <host_ipv6>}
      next
    end
  next
end
```

Variable	Description	Default
<protected-hosts_name>	Type the name of a new or existing group of protected hosts. The maximum length is 35 characters. To display the list of existing groups, type: edit ?	No default.
default-action {allow deny}	Select whether to accept or deny HTTP requests whose Host: field does not match any of the host definitions that you will add to this protected hosts group.	allow
<protected-host_index>	Type the index number of a protected host within its group. The valid range is from 1 to 9,223,372,036,854,775,807. Each host-list can contain up to 64 IP addresses and/or fully qualified domain names (FQDNs).	No default.
action {allow deny}	Select whether to accept or deny HTTP requests whose Host: field matches the host definition in host {<host_ipv4> <host_fqdn> <host_ipv6>} .	allow
host {<host_ipv4> <host_fqdn> <host_ipv6>}	Type the IP address or FQDN of a virtual or real web host, as it appears in the Host: field of HTTP headers, such as <code>www.example.com</code> . The maximum length is 255 characters. If clients connect to your web servers through the IP address of a virtual server on the FortiWeb appliance, this should be the IP address of that virtual server or any domain name to which it resolves, not the actual IP address of the web server. For example, if a virtual server 10.0.0.1/24 forwards traffic to the physical server 192.168.1.1, for protected hosts, you would enter: <ul style="list-style-type: none"> 10.0.0.1, the address of the virtual server www.example.com, the domain name that resolves to the virtual server 	No default.

Example

This example configures a protected hosts group named `example_com_hosts` that contains a web site's domain names and its IP address in order to match HTTP requests regardless of which form they use to identify the host.

```
config server-policy allow-hosts
  set default-action deny
  edit example_com_hosts
    config host-list
      edit 0
        set host example.com
      next
      edit 1
        set host www.example.com
      next
      edit 2
        set host 10.0.0.1
      next
    end
  next
end
```

Related topics

- [config server-policy policy](#)
- [config waf allow-method-exceptions](#)
- [config waf allow-method-policy](#)
- [config waf input-rule](#)
- [config waf signature](#)
- [config waf start-pages](#)
- [config waf page-access-rule](#)
- [config waf hidden-fields-rule](#)

server-policy custom-application application-policy

Some web applications build URLs differently than expected by FortiWeb, which causes FortiWeb to create incorrect auto-learning data.

To solve this kind of problem, FortiWeb uses application policy plug-ins that recognize the non-standard application URLs so that the auto-learning profile can work properly.

First create a URL interpreter (see [“server-policy custom-application url-replacer” on page 110](#)) and then use this command to create an application policy to use it.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy custom-application application-policy
  edit <policy_name>
    config rule-list
      edit <entry_index>
        set plugin-name <url-replacer_name>
        set type {URL_Replacer}
      next
    end
  next
end
```

Variable	Description	Default
<policy_name>	Type the name of a new or existing application policy. The maximum length is 35 characters. To display the list of existing policies, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual rule in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
plugin-name <url-replacer_name>	Type the name of an existing URL interpreter. The maximum length is 35 characters.	No default.
type {URL_Replacer}	Type the name of the plug-in type. (Currently, only the URL_Replacer option is supported.)	URL_Replacer

Example

This example adds two existing URL replacer plug-ins to an application policy.

```
config server-policy custom-application application-policy
  edit replacer-policy1
```

```
config rule-list
  edit 1
    set plugin-name url-replacer1
  next
  edit 2
    set plugin-name url-replacer2
  next
end
next
end
```

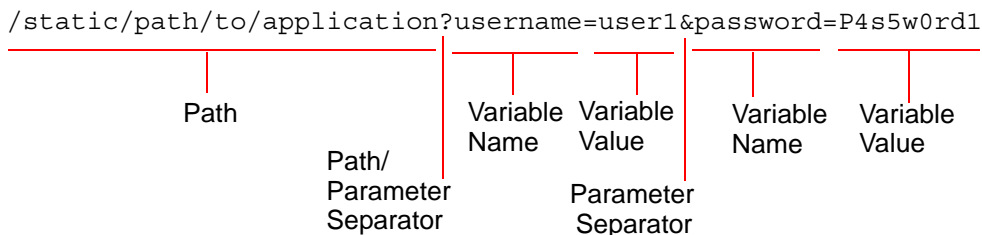
Related topics

- [config server-policy custom-application url-replacer](#)
- [config waf web-protection-profile autolearning-profile](#)

server-policy custom-application url-replacer

When web applications have dynamic URLs or unusual parameter styles, you **must** adapt auto-learning to recognize them.

By default, auto-learning assumes that your web applications use the most common URL structure:



- All parameters follow after a **question mark** (?). They do not follow a hash (#) or other separator character.
- If there are multiple name-value pairs, each pair is separated by an **ampersand** (&). They are not separated by a semi-colon (;) or other separator character.
- All paths before the question mark (?) are **static** — they do not change based upon input, blending the path with parameters (sometimes called a dynamic URL).

For example, the page at:

`/app/main`

always has that same path. After a person logs in, the page's URL **doesn't** become:

`/app/marco/main`

or

`/app#deepa`

For another example, the URL does **not** dynamically reflect inventory, such as:

`/app/sprockets/widget1024894`

Some web applications, however, embed parameters within the path structure of the URL, or use unusual or non-uniform parameter separator characters. **If you do not configure URL replacers for such applications, it can cause your FortiWeb appliance to gather auto-learning data incorrectly.** This can cause the following symptoms:

- Auto-learning reports do not contain a correct URL structure.
- URL or parameter learning is endless.
- When you generate a protection profile from auto-learning, it contains many more URLs than actually exist, because auto-learning cannot predict that the URL is actually dynamic.
- Parameter data is not complete, despite the fact that the FortiWeb appliance has seen traffic containing the parameter.

For example, with Microsoft Outlook Web App (OWA), the user's login name could be embedded within the path structure of the URL, such as:

`/owa/tom/index.html`

`/owa/mary/index.html`

instead of suffixed as a parameter, such as:

`/owa/index.html?username=tom`

`/owa/index.html?username=mary`

Auto-learning would continue to create new URLs as new users are added to OWA. Auto-learning would also expend extra resources learning about URLs and parameters that are actually the same. Additionally, auto-learning may not be able to fully learn the application structure, as each user may not request the same URLs.

To solve this, you would use this command and [config server-policy custom-application application-policy](#) to apply a URL replacer that recognizes the user name within the OWA URL as if it were a standard, suffixed parameter value so that auto-learning can function properly.

For example, if the URL is:

```
/application/value
```

and the URL replacer settings are:

Setting name	Value
type {pre-defined custom-defined}	custom-defined
url "<original-url_str>"	(/application/) ([^/]+\.\. [^/]+)
new-url <new-url_str>	\$0
param <value_str>	\$1
new-param <replaced-param_name>	setting

then the URL will be interpreted by auto-learning as:

```
/application?setting=value
```

To apply interpret non-standard URLs:

- 1 Create the custom URL replacer.
- 2 Add the URL replacer to a custom application policy see [“config server-policy custom-application application-policy” on page 108](#).
- 3 Apply the custom application policy in an auto-learning profile (see [“config waf web-protection-profile autolearning-profile” on page 387](#)).
- 4 Finally, apply the auto-learning profiles in a server policy (see [“config server-policy policy” on page 140](#)).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy custom-application url-replacer
edit <interpreter_name>
    set type {pre-defined | custom-defined}
    set app-type {jsp | owa-2003}
    set url "<original-url_str>"
```

```

    set new-url <new-url_str>
    set param <value_str>
    set new-param <replaced-param_name>
  next
end

```

Variable	Description	Default
<interpreter_name>	Type the name of a new or existing URL interpreter. The maximum length is 35 characters. To display the list of existing URL interpreter, type: edit ?	No default.
type {pre-defined custom-defined}	Select either: <ul style="list-style-type: none"> pre-defined — Use one of the predefined URL replacers for well-known web applications, which you select in <code>app-type {jsp owa-2003}</code>. custom-defined — Define your own URL replacer by configuring <code>url "<original-url_str>", new-url <new-url_str>, param <value_str>, and new-param <replaced-param_name>.</code> 	pre-defined
app-type {jsp owa-2003}	If type is pre-defined, select which predefined URL interpreter to use, either: <ul style="list-style-type: none"> jsp — Use the URL replacer designed for Java server pages (JSP) web applications, where parameters are often separated by semi-colons (;). owa-2003 — User the URL replacer designed for Microsoft Outlook Web App (OWA) 2003, where user name and directory parameters are often embedded in the URL. 	jsp

Variable	Description	Default
url "<original-url_str>"	<p>Type a regular expression, such as <code>^/(.*)/(.*)\$</code>, matching all and only the URLs to which the URL replacer should apply.</p> <p>The pattern does not require a backslash (<code>/</code>). However, it must at least match URLs that begin with a slash as they appear in the HTTP header, such as <code>/index.html</code>. Do not include the domain name, such as <code>www.example.com</code>.</p> <p>This setting is used only if <code>type</code> is <code>custom-defined</code>. The maximum length is 255 characters.</p> <p>Note: Auto-learning consider URLs up to approximately 180 characters long (assuming single-byte character encoding, after FortiWeb has decoded any nested hexadecimal or other URL encoding — therefore, the limit is somewhat dynamic). If the URL is greater than that buffer size, auto-learning will not be able to learn it, and so will ignore it. No event log will be created in this case.</p> <p>Note: If this URL replacer will be used sequentially in its set of URL replacers, instead of being mutually exclusive, this regular expression should match the URL produced by the previous interpreter, not the original URL from the request.</p>	No default.
new-url <new-url_str>	<p>Type either a literal URL, such as <code>/index.html</code>, or a regular expression with a back-reference (such as <code>/§1</code>) defining how the URL will be interpreted.</p> <p>This setting is used only if <code>type</code> is <code>custom-defined</code>. The maximum length is 255 characters.</p> <p>Note: Back-references can only refer to capture groups (parts of the expression surrounded with parentheses) within the same URL replacer. Back-references cannot refer to capture groups in other URL replacers.</p>	No default.

Variable	Description	Default
param <value_str>	Type either the parameter's literal value, such as user1, or a back-reference (such as /\$0) defining how the value will be interpreted. This setting is used only if type is custom-defined. The maximum length is 255 characters.	No default.
new-param <replaced-param_name>	Type either the parameter's literal name, such as username, or a back-reference (such as \$2) defining how the parameter's name will be interpreted in the auto-learning report. This setting is used only if type is custom-defined. The maximum length is 255 characters. Note: Back-references can only refer to capture groups (parts of the expression surrounded with parentheses) within the same URL replacer. Back-references cannot refer to capture groups in other URL replacers.	No default.

Example

This example assumes the HTTP request URL from a client is /mary/login.asp. The URL replacer interprets the URL to be /login.asp?username=mary.

```
config server-policy custom-application url-replacer
  edit url-replacer1
    set type custom-defined
    set url ^/(.*)/(.*)$
    set new-url /$1
    set param $0
    set new-param username
  next
end
```

Related topics

- [config server-policy custom-application application-policy](#)

server-policy dserver

Use this command to configure domain servers.

Domain servers use a domain name to define an individual server or a member of a server farm that is the ultimate destination of traffic received by the FortiWeb appliance at a virtual server address, and to which the FortiWeb appliance will forward traffic after applying the protection profile and other policy settings.



Alternatively, you can define your web servers using IP addresses. For details, see [“config server-policy pserver” on page 154](#).

To apply domain servers, select them within a server policy or a server farm that is selected in a policy. For details, see [“config server-policy policy” on page 140](#) or [“config server-policy pserver” on page 154](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy dserver
  edit <domain-server_name>
    set domain <server_fqdn>
    set status {enable | disable}
  next
end
```

Variable	Description	Default
<domain-server_name>	Type the name of a new or existing domain server definition. The maximum length is 35 characters. To display the list of existing domain server definitions, type: <code>edit ?</code>	No default.
status {enable disable}	Enable to forward connections accepted by the policy to the physical server.	No default.
domain <server_fqdn>	Type the domain name of a server, such as <code>www.example.com</code> . The maximum length is 255 characters.	No default.

Example

This example configures a domain server named `www.example.com`.

```
config server-policy dserver
  edit main-domain
    set domain www.example.com
```

```
        set status enable
    next
end
```

Related topics

- [config server-policy policy](#)
- [config server-policy pservers](#)
- [config server-policy pserver](#)

server-policy error-page

This command lets you name a customized error page to present to web clients when the FortiWeb appliance blocks a request because it violates a web protection rule. This only applies when the related action is `alert_deny`.



This command can only create the name of the error page to reference in a server policy. To upload a file to use for the error page, you must use the web UI.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy error-page
  edit <error-page_name>
  next
end
```

Variable	Description	Default
<error-page_name>	Type the name of a new or existing error page. The maximum length is 35 characters. To display the list of existing error page definitions, type: <code>edit ?</code>	No default.

Example

This example retrieves the name of the error page.

```
config server policy error-page
  edit ?
  ..
end
```

server-policy health

Use this command to configure server health checks.

Tests for server responsiveness (called “server health checks” in the web UI) poll web servers that are members of a server farm to determine their availability before forwarding traffic. Server health checks can use TCP, HTTP/HTTPS, or ICMP ECHO_REQUEST (ping).

The FortiWeb appliance will poll the server at the frequency set in the `interval <seconds_int>` option. If the appliance does not receive a reply within the timeout period, and you have configured the health check to retry, it attempts a health check again; otherwise, the server is deemed unresponsive. The FortiWeb appliance reacts to unresponsive servers by disabling traffic to that server until it becomes responsive.



If a real server will be unavailable for a long period, such as when a server is undergoing hardware repair, it is experiencing extended downtime, or when you have removed a server from the server farm, you may improve the performance of your FortiWeb appliance by disabling the real server, rather than allowing the server health check to continue to check for responsiveness. For details, see “[config server-policy pserver](#)” on page 154 and “[config server-policy dserver](#)” on page 115.

To apply server health checks, select them in a policy for use with a server farm. For details, see “[config server-policy policy](#)” on page 140.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see “[Permissions](#)” on page 47.

Syntax

```
config server-policy health
edit <health-check_name>
    set type {http | ping | tcp}
    set interval <seconds_int>
    set retry-times <retries_int>
    set time-out <seconds_int>
    set url-path <request_str>
    set regular <regex_pattern>
```

```

set trigger <trigger-policy_name>
next
end

```

Variable	Description	Default
<health-check_name>	Type the name of the server health check. The maximum length is 35 characters. To display the list of existing server health checks, type: edit ?	No default.
type {http ping tcp}	Type either: <ul style="list-style-type: none"> • http — Send an HTTP/HTTPS request, and listen for an HTTP/HTTPS response code 200 OK and page content matching url-path <request_str> indicating responsiveness, or timeout indicating that the host is not responsive. The protocol used depends on whether you enable ssl {enable disable} for that server in the server farm. • ping — Send ICMP type 8 (ECHO_REQUEST) and listen for either ICMP type 0 (ECHO_RESPONSE) indicating responsiveness, or timeout indicating that the host is not responsive. • tcp — Send TCP SYN and listen for either TCP SYN ACK indicating responsiveness, or timeout indicating that the host is not responsive. 	ping
interval <seconds_int>	Type the number of seconds between each server health check. The valid range is from 1 to 10 seconds.	5
retry-times <retries_int>	Type the number of times, if any, a failed health check will be retried before the server is determined to be unresponsive. The valid range is from 1 to 10 retries.	5
time-out <seconds_int>	Type the number of seconds which must pass after the server health check to indicate a failed health check. The valid range is from 1 to 10 seconds.	10
regular <regex_pattern>	Type the content that must be present in the HTTP reply to indicate proper server connectivity. You can use a regular expression. The maximum length is 255 characters. This option appears only when type is http.	No default.

Variable	Description	Default
trigger <trigger-policy_name>	Type the name of the trigger to apply when the health check detects a failed server (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
url-path <request_str>	Type the URL, such as /index.html, that will be used in the HTTP/HTTPS GET request to verify the responsiveness of the server. If the web server successfully returns this URL, and its content matches your expression in regular <regex_pattern> , it is considered to be responsive. This setting is available when type is http.	No default.

Example

This example configures a server health check that periodically requests the main page of the web site, /index. If a physical server does not successfully return that page (which contains the word “About”) every five seconds (the default), and fails the check at least three times in a row, it will be deemed unresponsive and the FortiWeb appliance will forward subsequent HTTP requests to other physical servers in the server farm.

```
config server-policy health
  edit status_check1
    set retry-times 3
    set type http
    set url-path "/index"
    set regular "About"
    set trigger-policy "notification-servers1"
  next
end
```

Related topics

- [config server-policy pservers](#)
- [config server-policy policy](#)
- [config log trigger-policy](#)

server-policy http-content-routing-policy

Use this command to configure HTTP header-based routing.

Instead of forwarding requests to back-end servers based upon load or connection distribution at the TCP/IP layers, you can forward them based upon headers in the HTTP layer.

HTTP header-based routes define how FortiWeb routes requests to specific back-end web servers in your server farm based on one or more of the following HTTP header elements:

- URL
- cookie
- Host : field

This can be useful if specific web applications, functions, or host names are divided, and each served only by a specific web server on the back end — that is, each web server in the server farm is **not** identical, but is specialized, such as:

- 192.168.0.1 — Hosts the web site and blog
- 192.168.0.2 — Hosts movie clips and multimedia
- 192.168.0.3 — Hosts the shopping cart

If you have configured request rewriting, configure HTTP content-based routing using the original request URL and/or Host : name, as it appears **before** FortiWeb has rewritten it. For more information on rewriting, see [“config waf url-rewrite url-rewrite-policy” on page 379](#).

To apply your HTTP-based routes, select them when you configure the server farm (see [“server-policy pservers” on page 156](#)).

To use this command, your administrator account’s access control profile must have either w or rw permission to the traroutegrp area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy http-content-routing-policy
  edit <routing-policy_name>
    config content-routing-list
      edit <entry_index>
        set host-status {enable | disable}
        set host {<host_fqdn> | <host_ipv4>}
        set url-type {Regular-expression | Simple-string}
        set request-url "<url_str>"
        set cookie-name <cookie-name_str>
        set cookie-type {Regular-expression | Simple-string}
        set cookie-value <cookie-val_str>
        set is-essential {yes | no}
      next
    next
  next
```

```

end
next
end

```

Variable	Description	Default
<routing-policy_name>	Type the name of the HTTP content routing policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
<entry_index>	Type the index number of the individual rule in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host-status {enable disable}	Enable to perform HTTP Host : header name-based routing.	disable
host {<host_fqdn> <host_ipv4>}	Type either the IP address or host name of the destination server in the server farm to which the appliance will route matching HTTP requests. The maximum length is 255 characters. This setting is available only if host-status is enabled.	No default.
url-type {Regular-expression Simple-string}	Select the method used to match the URL upon which routing will take place. If matching is done according to host, use regular-expression.	simple-string
request-url "<url_str>"	Depending on url-type, type either a URL or a pattern defining a set of URLs that will match this policy and be routed. The maximum length is 255 characters. If matching by host, add \ / (a back slash and forward slash with no space between) in the URL pattern. For example: \ /example.com	No default.
<cookie-name_str>	Type the name of the cookie (for example, sessid) to use for load balancing, as it appears in the HTTP header. For example, web application's session cookie (for session persistence), or a cookie embedded by traffic controller software on one of the servers.	No default.
cookie-type {Regular-expression Simple-string}	Specify whether the value of cookie-value field is a literal value (simple-string), or a regular expression that is designed to match multiple values (regular-expression).	Simple-string

Variable	Description	Default
<code><cookie-val_str></code>	<p>If the value of <code>cookie-type</code> is <code>simple-string</code>, specify the literal value (for example, <code>TRUE</code>) that the cookie must contain in order to match the rule.</p> <p>If the value of <code>cookie-type</code> is <code>regular-expression</code>, enter a regular expression (for example, <code>hash[a-zA-F0-7]*</code>) that matches all and only the cookie values to which the rule applies.</p>	No default.
<code>is-essential {yes no}</code>	<p>To specify that requests require the specified cookie, enter <code>yes</code>.</p> <p>Requests can lack a <code>Cookie:</code> field for several reasons, such as if the user is initiating a session, has cleared their browser's cookie cache, or if the web application itself has reset the session, such as after a logout or password change. In those cases, the field cannot be tested for a matching value.</p>	no

Example

This example configures an HTTP content routing policy to route URL requests for `www.example.com/school` to a physical server in the server farm with IP address `10.5.5.12`. The content routing is based on matching a regular expression in a URL and/or cookie.

```
config server-policy http-content-routing-policy
  edit content_routing_policy1
    set host-status enable
    set host 10.5.5.12
    set request-url \/example.com
    set cookie-name sessid
    set cookie-type Regular-expression
    set cookie-value hash{a-zA-F0-7}*
    set is-essential no
  next
end
```

Related topics

- [config server-policy pservers](#)
- [config server-policy policy](#)
- [config waf url-rewrite url-rewrite-policy](#)

server-policy pattern custom-data-type

Use this command to configure custom data types to augment the predefined data types. You can add custom data types to input rules to define the data type of an input, and to auto-learning profiles to detect valid input parameters.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pattern custom-data-type
  edit <custom-data-type_name>
    set expression <regex_pattern>
  next
end
```

Variable	Description	Default
<custom-data-type_name>	Type the name of the custom data type. The maximum length is 35 characters. To display the list of existing types, type: edit ?	No default.
expression <regex_pattern>	Type a regular expression that defines the data type. It should match all data of that type, but nothing else. The maximum length is 2,071 characters.	No default.

Example

This example configures two custom data types.

```
config server-policy pattern custom-data-type
  edit "Level 3 Password-custom"
    set expression "^aaa"
  next
  edit "Custom Data Type 1"
    set expression "^555"
  next
end
```

Related topics

- [config server-policy pattern data-type-group](#)

server-policy pattern custom-global-white-list-group

Use this command to configure objects that will be exempt from scans.

When enabled, whitelisted items are **not** flagged as potential problems, nor incorporated into auto-learning data. This feature reduces false positives and improves performance.

To include white list items during policy enforcement and auto-learning reports, you must first disable them in the global white list.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pattern custom-global-white-list-group
edit <entry_index>
    set status {enable | disable}
    set type {Cookie | Parameter | URL}
    set domain <cookie_fqdn>
    set name <name_str>
    set path <url_str>
    set request-type {plain | regular}
    set request-file <url_str>
next
end
```

Variable	Description	Default
<entry_index>	Type the index number of the individual rule in the table. The valid range is from 1 to 9,223,372,036,854,775,807.	No default.
status {enable disable}	Enable to exempt this object from all scans.	enable
type {Cookie Parameter URL}	Indicate the type of the object. Depending on your selection, the remaining settings vary.	URL
domain <cookie_fqdn>	Type the partial or complete domain name or IP address as it appears in the cookie, such as: <ul style="list-style-type: none">www.example.com.google.com10.0.2.50 If clients sometimes access the host via IP address instead of DNS, create white list objects for both. This setting is available if type is set to Cookie. Caution: Do not whitelist untrusted subdomains that use vulnerable cookies. It could compromise the security of that domain and its network.	No default.

Variable	Description	Default
name <name_str>	<p>Depending on your selection in type {Cookie Parameter URL}, either:</p> <ul style="list-style-type: none"> type the name of the cookie as it appears in the HTTP request, such as NID. type the name of the parameter as it appears in the HTTP URL or body, such as rememberme. <p>This setting is available if <code>type</code> is set to <code>Cookie</code> or <code>Parameter</code>.</p>	No default.
path <url_str>	<p>Type the path as it appears in the cookie, such as <code>/</code> or <code>/blog/folder</code>.</p> <p>This setting is available if <code>type</code> is set to <code>Cookie</code>.</p>	No default.
request-type {plain regular}	<p>Indicate whether the request-file <url_str> field will contain a literal URL (<code>plain</code>), or a regular expression designed to match multiple URLs (<code>regular</code>).</p> <p>This setting is available if <code>type</code> is set to <code>URL</code>.</p>	plain
request-file <url_str>	<p>Depending on your selection in the request-type {plain regular} field, enter either:</p> <ul style="list-style-type: none"> the literal URL, such as <code>/robots.txt</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a backslash (<code>/</code>). a regular expression, such as <code>^/*\.html</code>, matching all and only the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a backslash, such as <code>/index.html</code>. <p>Do not include the domain name, such as <code>www.example.com</code>.</p> <p>This setting is available if <code>type</code> is set to <code>URL</code>.</p>	

Example

This example exempts requests for robots.txt from most scans.

```
config server-policy pattern custom-global-white-list-group
edit 1
    set request-file /robots.txt
next
end
```

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile autolearning-profile](#)

server-policy pattern custom-susp-url

Use this command to configure custom suspicious URL requests to augment the list of predefined suspicious URL requests. You can add custom suspicious URLs to a custom suspicious URL rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pattern custom-susp-url
  edit <custom-susp-url_name>
    set expression <url_pattern>
  next
end
```

Variable	Description	Default
<custom-susp-url_name>	Type the name of the custom URL. The maximum length is 35 characters. To display the list of existing URLs, type: edit ?	No default.
expression <url_pattern>	Type either a simple string or a regular expression to defines the custom URL request to check for. The maximum length is 2,071 characters.	No default.

Example

This example configures a custom suspicious URL named `Suspicious-URL 1` and defines the custom expression associated with that suspicious URL.

```
config server-policy pattern custom-susp-url
  edit "Suspicious URL 1"
    set expression "^/schema.xml$"
  next
end
```

Related topics

- [config server-policy pattern suspicious-url-rule](#)

server-policy pattern custom-susp-url-rule

Use this command to add one or more existing custom suspicious URLs to a custom suspicious URL rule.

Custom suspicious URL rules can augment the predefined suspicious URL rules. You can add custom suspicious URL rules to input rules.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pattern custom-susp-url-rule
  edit <rule_name>
    config type-list
      edit <entry_index>
        set custom-susp-url <suspicious-url_name>
      next
    end
  next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
custom-susp-url <suspicious-url_name>	Type the name of an existing custom URL already defined using config server-policy pattern custom-susp-url . The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.

Example

This example configures a custom suspicious URL rule using an existing custom suspicious URL.

```
config server-policy pattern custom-susp-url-rule
  edit "Suspicious Rule 1"
    config type-list
      edit 1
        set custom-susp-url "Suspicious URL 1"
      next
    end
  next
end
```


Related topics

- [config server-policy pattern custom-susp-url](#)

server-policy pattern data-type-group

Use this command to configure data type groups.

A data type group selects a subset of one or more predefined data types. Each of those entries in the data type group defines a type of input that the FortiWeb appliance should attempt to recognize and track in HTTP sessions when gathering data for an auto-learning profile.

For example, if you include the `Email` data type in the data type group, auto-learning profiles that use the data type group might discover that your web applications use a parameter named `username` whose value is an email address.

If you know that your network's HTTP sessions do not include a specific data type, omit it from the data type group to improve performance. The FortiWeb appliance will not expend resources scanning traffic for that data type.

Data type groups are used by auto-learning profiles. For details, see [“config server-policy policy” on page 140](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pattern data-type-group
edit <data-type-group_name>
    config type-list
        edit <entry_index>
            set data-type {Address | Canadian_Post_code |
                Canadian_Province_Name | Canadian_SIN | China_Post_Code |
                Country_Name | Credit_Card_Number | Danmark_Postalcode |
                Dates_and_Times | Email | GPA | GUID | ip_address |
                Indian_Vehicle_Number | Italian_mobile_phone |
                Kuwait_Civil_ID | L1_Password | L2_Password |
                Markup_or_Code | Microsoft_product_key | NINO |
                Netherlands_Postcode | Num | personal_name | Phone |
                Quebec_Postal_Code | String | Swedish_personal_number |
                Swedish_Postalcode | UAE_land_phone | UK_Bank_code |
                UK_postcode | US_SSN | US_State_Name | US_Street_Address |
                US_Zip_Code | Unix_device_name | Uri | Windows_file_name}
        next
    end
next
end
```

Variable	Description	Default
<data-type-group_name>	Type the name of the data type group. The maximum length is 35 characters. To display the list of existing groups, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.

Variable	Description	Default
data-type {Address Canadian_Post_code Canadian_Province_Name Canadian_SIN China_Post_Code Country_Name Credit_Card_Number Danmark_Postalcode Dates_and_Times Email GPA GUID ip_address Indian_Vehicle_Number Italian_mobile_phone Kuwait_Civil_ID L1_Password L2_Password Markup_or_Code Microsoft_product_key NINO Netherlands_Postcode Num personal_name Phone Quebec_Postal_Code String Swedish_personal_number Swedish_Postalcode UAE_land_phone UK_Bank_code UK_postcode US_SSN US_State_Name US_Street_Address US_Zip_Code Unix_device_name Uri Windows_file_name}	<p>For each data-type entry, enter one of the following predefined data types exactly as shown (available options may vary due to FortiGuard updates):</p> <ul style="list-style-type: none"> Address — Canadian postal codes and United States ZIP code and ZIP + 4 codes. Canadian_Post_code — Canadian postal codes such as K2H 7B8 or k2h7b8. Does not match hyphenations such as K2H-7B8. Canadian_Province_Name — Modern and older names and abbreviations of Canadian provinces in English, as well as some abbreviations in French, such as Quebec, IPE, Sask, and Nunavut. Does not detect province names in French, such as Québec. Canadian_SIN — Canadian Social Insurance Numbers (SIN) such as 123-456-789. China_Post_Code — Chinese postal codes such as 610000. Country_Name — Country names, codes, and abbreviations in English characters, such as CA, Cote d'Ivoire, Brazil, Russian Federation, Brunei, and Dar el Salam. Credit_Card_Number — American Express, Carte Blanche, Diners Club, enRoute, Japan Credit Bureau (JCB), Master Card, Novus, and Visa credit card numbers. Danmark_Postalcode — Danish postal code ("postnumre") such as DK-1499 and dk-1000. Does not match codes that are not prefixed by "DK-", nor numbers that do not belong to the range of valid codes, such as 123456 or dk 12. Dates_and_Times — Dates and times in various formats such as +13:45 for time zone offsets, 1:01 AM, 1am, 23:01:01, and 01.01.30 AM for times, and 31.01.2009, 31/01/2009, 01/31/2000, 2009-01-3, 31-01-2009, 1-31-2009, 01 Jan 2009, 01 JAN 2009, 20-Jan-2009 and February 29, 2009 for dates. Email — Email addresses such as admin@example.com GPA — A student's grade point average, such as 3.5, based upon the 0.0-to-4.0 point system, where an "A" is worth 4 points and an "F" is worth 0 points. Does not match GPAs weighted on the 5 point scale for honors, IB, or AP courses, such as 4.1. The exception is 5.5, which it will match. GUID — A globally unique identifier used to identify partition types in the hard disk's master boot record (MBR), such as BFDB4D31-3E35-4DAB-AFCA-5E6E5C8F61EA. Partition types are relevant on computers which boot via EFI, using the MBR, instead of an older-style BIOS. 	No default.

Variable	Description	Default
data-type {Address Canadian_Post_code Canadian_Province_Name Canadian_SIN China_Post_Code Country_Name Credit_Card_Number Danmark_Postalcode Dates_and_Times Email GPA GUID ip_address Indian_Vehicle_Number Italian_mobile_phone Kuwait_Civil_ID L1_Password L2_Password Markup_or_Code Microsoft_product_key NINO Netherlands_Postcode Num personal_name Phone Quebec_Postal_Code String Swedish_personal_number Swedish_Postalcode UAE_land_phone UK_Bank_code UK_postcode US_SSN US_State_Name US_Street_Address US_Zip_Code Unix_device_name Uri Windows_file_name}	<p>For each data-type entry, enter one of the following predefined data types exactly as shown (available options may vary due to FortiGuard updates):</p> <ul style="list-style-type: none"> Address — Canadian postal codes and United States ZIP code and ZIP + 4 codes. Canadian_Post_code — Canadian postal codes such as K2H 7B8 or k2h7b8. Does not match hyphenations such as K2H-7B8. Canadian_Province_Name — Modern and older names and abbreviations of Canadian provinces in English, as well as some abbreviations in French, such as Quebec, IPE, Sask, and Nunavut. Does not detect province names in French, such as Québec. Canadian_SIN — Canadian Social Insurance Numbers (SIN) such as 123-456-789. China_Post_Code — Chinese postal codes such as 610000. Country_Name — Country names, codes, and abbreviations in English characters, such as CA, Cote d'Ivoire, Brazil, Russian Federation, Brunei, and Dar el Salam. Credit_Card_Number — American Express, Carte Blanche, Diners Club, enRoute, Japan Credit Bureau (JCB), Master Card, Novus, and Visa credit card numbers. Danmark_Postalcode — Danish postal code ("postnumre") such as DK-1499 and dk-1000. Does not match codes that are not prefixed by "DK-", nor numbers that do not belong to the range of valid codes, such as 123456 or dk 12. Dates_and_Times — Dates and times in various formats such as +13:45 for time zone offsets, 1:01 AM, 1am, 23:01:01, and 01.01.30 AM for times, and 31.01.2009, 31/01/2009, 01/31/2000, 2009-01-3, 31-01-2009, 1-31-2009, 01 Jan 2009, 01 JAN 2009, 20-Jan-2009 and February 29, 2009 for dates. Email — Email addresses such as admin@example.com GPA — A student's grade point average, such as 3.5, based upon the 0.0-to-4.0 point system, where an "A" is worth 4 points and an "F" is worth 0 points. Does not match GPAs weighted on the 5 point scale for honors, IB, or AP courses, such as 4.1. The exception is 5.5, which it will match. GUID — A globally unique identifier used to identify partition types in the hard disk's master boot record (MBR), such as BFDB4D31-3E35-4DAB-AFCA-5E6E5C8F61EA. Partition types are relevant on computers which boot via EFI, using the MBR, instead of an older-style BIOS. 	No default.

Variable	Description	Default
	<ul style="list-style-type: none"> <code>ip_address</code> — A public or private IPv4 address, such as 10.0.0.1. Does not match IPv6 addresses. <code>Indian_Vehicle_Number</code> — An Indian Vehicle Registration Number, such as mh 12 bj 1780. <code>Italian_mobile_phone</code> — Italian mobile phone numbers with the prefix for international calls, such as +393471234567, or without, such as 3381234567. Does not match numbers with a dash or space after the area code, nor VoIP or land lines. <code>Kuwait_Civil_ID</code> — Personal identification number for Kuwait, such as 273032401586. Must begin with 1, 2, or 3, and follow all other number patterns for valid civil IDs. <code>L1_Password</code> — A string of at least 6 characters, with one or more each of lower-case characters, upper-case characters, and digits, such as aBc123. Level 1 passwords are “weak” passwords, generally easier to crack than level 2 passwords. <code>L2_Password</code> — A strong password — string of at least 8 characters, with one or more each of lower-case characters, upper-case characters, digits, and special characters, such as aBc123\$%. <code>Markup_or_Code</code> — HTML comments, wiki code, hexadecimal HTML color codes, quoted strings in VBScript and ANSI SQL, SQL statements, and RTF bookmarks such as: <ul style="list-style-type: none"> <code>#00ccff, <!--A comment.--></code> <code>[link url="http://example.com/url?var=A&var2=B"]</code> <code>SELECT * FROM TABLE</code> <code>{*\bkmkstart TagAmountText}</code> Does not match ANSI escape codes, which are instead detected as strings. <code>Microsoft_product_key</code> — An alphanumeric key for activation of Microsoft software, such as ABC12-34DEF-GH567-IJK89-LM0NP. Does not match keys which are non-hyphenated, nor where letters are not capitalized. <code>Netherlands_Postcode</code> — Netherlands postal codes (“postcodes”) such as 3000 AA or 3000AA. Does not match postal codes written in lower-case letters, such as 3000aa. <code>NINO</code> — A United Kingdom National Insurance Number (NINO), such as AB123456D. Does not match NINOs written in lower-case letters, such as ab123456d. 	

Variable	Description	Default
	<ul style="list-style-type: none"> • <code>Num</code> — Numbers in various monetary, decimal, comma-separated value (CSV) and other formats such as 123, +1.23, \$1,234,567.89, 1'235.140, and -123.45e-6. Does not detect hexadecimal numbers, which are instead detected as strings or code, and Social Security Numbers, which are instead detected as strings. • <code>personal_name</code> — A person's full or abbreviated name in English. It can contain punctuation, such as A.J. Schwartz, Jean-Pierre Ferko, or Jane O'Donnell. Does not match names written in other languages with accented Latin characters, hanzu, kanji, or hangul, such as Renée Wächter or 林美. • <code>Phone</code> — Australian, United States, and Indian phone numbers in various formats such as (123)456-7890, 1.123.456.7890, 0732105432, and +919847444225. • <code>Quebec_Postal_Code</code> — Postal codes written in the style sometimes used by Quebecers, with hyphens between the two parts, such as h2j-3c4 or H2J-3C4. • <code>String</code> — Character strings such as alphanumeric words, credit card numbers, United States Social Security Numbers (SSN), UK vehicle registration numbers, ANSI escape codes, and hexadecimal numbers in formats such as user1, 123-45-6789, ABC 123 A, 4125632152365, [32mHello, and 8ECCA04F. • <code>Swedish_Postalcode</code> — Postal codes ("postnummer") for Sweden, with or without spaces or hyphens, such as S 751 70, s75170, or S-751-70. Requires the initial S or s letter. Does not match invalid postal codes such as ones that begin with a 0, or ones that do not begin with the letter S or s. • <code>Swedish_personal_number</code> — Personal identification number ("personnummer") for Sweden, such as 19811116-7845. Must be hyphenated. Does not match PINs for persons whose age is 100 or greater. • <code>UAE_land_phone</code> — Telephone number for the United Arab Emirates, such as 04 - 3452499 or 04 3452499. Does not match phone numbers beginning with 01 or 08. • <code>UK_Bank_code</code> — Bank sort codes for the United Kingdom, such as 09-01-29. Must be hyphenated. • <code>UK_postcode</code> — Postal codes for the United Kingdom, with or without spaces, such as SW1A 2AA or SW1A2AA. • <code>Unix_device_name</code> — Standard Linux or UNIX non-loopback wired Ethernet network interface names, such as eth0. Does not match names for any other type of device, such as lo, hdda, or ppp. 	

Variable	Description	Default
	<ul style="list-style-type: none"> Uri — Uniform resource identifiers (URI) such as: http://www.example.com ftp://ftp.example.com mailto:admin@example.com US_SSN — United States Social Security Numbers (SSN) such as 123-45-6789. US_State_Name — United States state names and modern postal abbreviations such as HI and Wyoming. Does not detect older postal abbreviations such as Fl. or Wyo. US_Street_Address — United States city and street address, possibly including an apartment or suite number. City and street may be either separated with a space or written on two lines according to US postal conventions, such as: 123 Main Street Suite #101 Honolulu, HI 10001 Does not match: <ul style="list-style-type: none"> ZIP + 4 codes that include spaces, or do not have a hyphen (e.g. “10001 - 1111” or “10001 1111”) city abbreviations of 2 characters (e.g. “NY” instead of “NYC”) Washington D.C. addresses <ul style="list-style-type: none"> multiline addresses on Mac OS X, Linux or Unix computers unabbreviated state names (e.g. “Delaware”) addresses ending with the country (e.g. “USA”) addresses beginning with numbers written as words (e.g. “Seven Main Street” instead of “7 Main Street”) US_Zip_Code — United States ZIP code and ZIP + 4 codes such as 34285-3210. Windows_file_name — A valid windows file name, such as Untitled.txt. Does not match file extensions, or file names without their extensions. <p>To display available options, type:</p> <pre>set data-type ?</pre> <p>Note: The web UI displays the regular expressions that define each predefined data type. For details, see the FortiWeb Administration Guide.</p>	

Example

This example configures a data type group named `data-type-group1` that detects addresses and phone numbers when an auto-learning profile uses it.

```
config server-policy pattern data-type-group
  edit data-type-group1
```

```
config type-list
  edit 1
    set data-type Address
  next
  edit 2
    set data-type Phone
  next
end
next
end
```

Related topics

- [config waf web-protection-profile autolearning-profile](#)

server-policy pattern suspicious-url-rule

Use this command to add one or more predefined suspicious URL rules to a suspicious URL rule group.

Each entry in a suspicious URL group defines a type of URL that the FortiWeb appliance considers to be possibly malicious when gathering data for an auto-learning profile.

HTTP requests for URLs typically associated with administrative access to your web applications or web server, for example, may be malicious if they originate from the Internet instead of your management LAN. You may want to discover such requests for the purpose of designing blacklist page rules to protect your web server.

If you know that your network's web servers are not vulnerable to a specific type of suspicious URL, such as if the URL is associated with attacks on Microsoft IIS web servers but all of your web servers are Apache web servers, omit it from the suspicious URL group to improve performance. The FortiWeb appliance will not expend resources scanning traffic for that type of suspicious URLs.

To see the regular expressions used in the predefined suspicious URL rules, in the web UI, go to *Auto Learn > Predefined Pattern > URL Pattern*.

Suspicious URL groups are used by auto-learning profiles. For details, see [“config server-policy policy” on page 140](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pattern suspicious-url-rule
edit <rule-group_name>
    config type-list
        edit <entry_index>
            set server-type { Abyss | Apache | Appweb | BadBlue |
                Blazix | Cherokee | ColdFusion | IIS | JBoss | Jetty |
                Jeus_WebContainer | LotusDomino | Tomcat | WebLogic |
                WebSEAL | WebSiphon | Xerver | ZendServer | aolserver |
                ghttpd | lighttpd | lilhttpd | localweb2000 | mywebserver |
                nginx | omnihttpd | samba | squid | svn | webshare | xeneo |
                xitami | zeus | zope}
        next
    end
    set custom-susp-url-rule <rule_name>
next
```

```

end
next
end

```

Variable	Description	Default
<rule-group_name>	Type the name of the suspicious URL rule group. The maximum length is 35 characters. To display the list of existing groups, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
server-type { Abyss Apache Appweb BadBlue Blazix Cherokee ColdFusion IIS JBoss Jetty Jeus_WebContainer LotusDomino Tomcat WebLogic WebSEAL WebSiphon Xerver ZendServer aolserver ghttpd lighttpd lilhttpd localweb2000 mywebserver nginx omnihttpd samba squid svn webshare xeneo xitami zeus zope }	For each rule index, select the type of the web server, application, or servlet. FortiWeb will detect attempts to access URLs that are usually sensitive for that software.	No default.
<rule_name>	Type the name of a custom suspicious URL rule (see “config server-policy pattern custom-susp-url-rule” on page 128).	

Example

This example configures a suspicious URL rule group named `suspicious-url-group1` that detects HTTP requests for administratively sensitive URLs for some common web servers that could represent attack attempts and includes a custom suspicious URL rule.

```

config server-policy pattern suspicious-url-rule
  edit suspicious-url-group1

```

```
config type-list
  edit 1
    set server-type Apache
  next
  edit 2
    set server-type Apache
  next
  edit 3
    set server-type Tomcat
  next
  edit 4
    set server-type WebLogic
  next
end
set custom-susp-url-rule "Suspicious URL 1"
next
end
```

Related topics

- [config waf web-protection-profile autolearning-profile](#)
- [config server-policy pattern custom-susp-url](#)

server-policy policy

Use this command to configure server policies.

The FortiWeb appliance applies only one server policy to each connection.

A policy will not be used while it is disabled, as indicated by `status {enable | disable}`.

Policy behavior varies by the operation mode. For details, see the [FortiWeb Administration Guide](#).



When you switch the operation mode, server policies will be deleted from the configuration file if they are not applicable in the current operation mode.

Before you can configure a server policy, you must first configure several policies and profiles:

- Configure a virtual server, a physical server, domain server or server farm.
- Configure a health check if needed by the server policy.
- To restrict traffic based upon which hosts you want to protect, configure a group of protected host names.
- If you want the FortiWeb appliance to gather auto-learning data, generate or configure an auto-learning profile and its required components.
- If you plan to authenticate users, you need to configure users, user groups, and authentication rules and policy, and include the policy in an inline web protection profile.
- To apply a web protection profile to a server policy, you must first configure them.
- If you want to use the FortiWeb appliance to apply SSL to connections instead of using physical servers, or if it must decrypt SSL connections in order to log them in offline protection mode or either of the transparent modes, you must also import a server certificate.
- Finally, if you want the FortiWeb appliance to verify the certificate provided by an HTTP client to authenticate themselves, you must also define a certificate verification rule.

For details, see:

- [config server-policy allow-hosts](#)
- [config server-policy vserver](#), [config server-policy pserver](#), [config server-policy dserver](#), [config server-policy pservers](#)
- [config server-policy health](#)
- [config user ldap-user](#), [config user local-user](#), [config user radius-user](#), [config user ntlm-user](#), [config user user-group](#), [config waf http-authen http-authen-rule](#), [config waf http-authen http-authen-policy](#)
- [config waf web-protection-profile inline-protection](#) (reverse proxy mode or either of the transparent modes), or [config waf web-protection-profile offline-protection](#) (offline protection mode)
- [config waf web-protection-profile autolearning-profile](#)
- [config system certificate local](#)
- [config system certificate verify](#)

You can use SNMP traps to notify you of policy status changes, or when a policy enforces your network usage policy. For details, see “[config system snmp community](#)” on page 234.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy policy
edit <policy_name>
    set server-type {domain | physical}
    set monitor-mode {enable | disable}
    set status {enable | disable}
    set deployment-mode {single-server | server-balance | http-
content-routing | offline-detection | transparent-servers}
    set allow-hosts <hosts_name>
    set block-port <port_int>
    set case-sensitive {enable | disable}
    set certificate <certificate_name>
    set client-certificate-forwarding {enable | disable}
    set comment "<comment_str>"
    set error-msg <message_str>
    set error-page <page_name>
    set error-page-code <status-code_int>
    set health <health-check_name>
    set intermediate-certificate-group <CA-group_name>
    set lb-algo {round-robin | weighted-round-robin | least-
connection | http-session-based-round-robin}
    set monitor-mode {enable | disable}
    set noparse {enable | disable}
    set http-pipeline {enable | disable}
    set persistence-timeout <timeout_int>
    set persistent-server-sessions <http-sessions_int>
    set pserver <pserver_name>
    set pserver-port <port_int>
    set pserver-sport <port_int>
    set pservers <server-farm_name>
    set server-connection-pool {enable | disable}
    set service <service_name>
    set https-service <service_name>
    set hsts-header {enable | disable}
    set hsts-max-age <timeout_int>
    set ssl-client-verify <verifier_name>
    set ssl-server {enable | disable}
    set vserver <vserver_name>
    set v-zone <bridge_name>
    set waf-autolearning-profile <profile_name>
    set web-protection-profile <profile_name>
    set syncookie {enable | disable}
```

```

    set half-open-threshold <packets_int>
  next
end

```

Variable	Description	Default
<policy_name>	Type the name of the policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
server-type {domain physical}	Select the server type. Note: Only the <code>physical</code> option is available in CLI. To configure a server policy for a domain server, you must use the web UI.	physical
monitor-mode {enable disable}	Enable to override deny and redirect actions defined in the server protection rules for the selected policy. This enables FortiWeb to log attacks without performing the deny or redirect action, and to collect more information to build an auto learning profile for the attack. Disable to allow attack deny/redirect actions to be performed as defined by the server protection rules	disable
status {enable disable}	Enable to allow the policy to be used when evaluating traffic for a matching policy. Note: You can use SNMP traps to notify you of changes to the policy's status. For details, see “config system snmp community” on page 234 .	No default.

Variable	Description	Default
<pre>deployment-mode {single-server server-balance http- content-routing offline-detection transparent-servers}</pre>	<p>Select one applicable distribution method that the FortiWeb appliance will use when forwarding connections accepted by this policy.</p> <ul style="list-style-type: none"> <code>single-server</code> — Forward connections to a single physical server. Also configure <code>pserver <pserver_name></code>, and <code>pserver-port <port_int></code>. This option is available only if the FortiWeb appliance is operating in reverse proxy mode. <code>server-balance</code> — Use a load-balancing algorithm when distributing connections amongst the physical servers in a server farm. If a physical server is unresponsive to the server health check, the FortiWeb appliance forwards subsequent connections to another physical server in the server farm. Also configure <code>lb-algo</code>, and <code>pservers <server-farm_name></code>. This option is available only if the FortiWeb appliance is operating in reverse proxy mode. <code>http-content-routing</code> — Use HTTP content routing to route HTTP requests to a specific web server in a server farm by specifying the host or URL and the request file. This option is available only if the FortiWeb appliance is operating in reverse proxy mode. <code>offline-detection</code> — Allow connections to pass through the FortiWeb appliance, and apply an offline protection profile. Also configure <code>health <health-check_name></code> and <code>pservers <server-farm_name></code>. This option is available only if the FortiWeb appliance is operating in offline protection mode. <code>transparent-servers</code> — Allow connections to pass through the FortiWeb appliance, and apply a protection profile. Also configure <code>pservers <server-farm_name></code>. This option is available when the FortiWeb appliance is operating in either of the transparent modes. <p>Depending on the types of topologies that the current operation mode supports, not all deployment modes may be available. For details, see the FortiWeb Administration Guide.</p>	No default.
<pre>allow-hosts <hosts_name></pre>	<p>Type the name of a protected hosts group to allow or reject connections based upon whether the <code>Host :</code> field in the HTTP header is empty or does or does not match the protected hosts group. The maximum length is 35 characters.</p> <p>To display the list of existing groups, type:</p> <pre>edit ?</pre> <p>If you do not select a protected hosts group, connections will be accepted or blocked based upon other criteria in the policy or protection profile, but regardless of the <code>Host :</code> field in the HTTP header.</p> <p>Note: Unlike HTTP 1.1, HTTP 1.0 does not require the <code>Host :</code> field. The FortiWeb appliance will not block HTTP 1.0 requests for lacking this field, regardless of whether or not you have selected a protected hosts group.</p>	No default.

Variable	Description	Default
block-port <port_int>	<p>Type the number of the physical network interface port from which to send TCP RST (reset) packets when a request violates the policy. The valid range varies by the number of physical ports on the NIC.</p> <p>For example, to send TCP RST from port1, type:</p> <pre>set block-port port1</pre> <p>This option is available only in offline protection mode.</p>	No default.
case-sensitive {enable disable}	<p>Enable to differentiate uniform resource locators (URLs) according to upper case and lower case letters for features that act upon the URLs in the headers of HTTP requests, such as start page rules, black list rules, white list rules, and page access rules.</p> <p>For example, when enabled, an HTTP request involving <code>http://www.Example.com/</code> would not match protection profile features that specify <code>http://www.example.com</code> (difference highlighted in bold).</p>	No default.
certificate <certificate_name>	<p>Type the name of the certificate that the FortiWeb appliance will use when encrypting or decrypting SSL-secured connections. The maximum length is 35 characters.</p> <p>To display the list of existing certificates, type:</p> <pre>edit ?</pre> <p>This option is used only if <code>https-service <service_name></code> is configured.</p>	No default.
client-certificate-forwarding {enable disable}	<p>Enable to include the X.509 personal certificate presented by the client during the SSL/TLS handshake, if any, in an X-Client-Cert: HTTP header when forwarding the traffic to the protected web server.</p> <p>FortiWeb will still validate the client certificate itself, but this can be useful if the web server requires the client certificate for the purpose of server-side identity-based functionality.</p> <p>This option appears only if <code>ssl-client-verify <verifier_name></code> is configured.</p>	disable
comment "<comment_str>"	<p>Type a description or other comment. If the comment is more than one word or contains special characters, surround the comment with double quotes ("). The maximum length is 63 characters.</p>	No default.
error-msg <message_str>	<p>Type an error message that FortiWeb will use to respond to blocked requests. Alternatively, configure <code>error-page <page_name></code>.</p> <p>The maximum length is 1,023 characters.</p>	No default.
error-page <page_name>	<p>Type the name of an existing, previously uploaded error page, if any, to use with this server policy. Alternatively, configure <code>error-msg <message_str></code>.</p> <p>The maximum length is 35 characters.</p> <p>To display the list of existing error pages, type:</p> <pre>edit ?</pre>	No default.

Variable	Description	Default
error-page-code <status-code_int>	<p>Type the HTTP status code that FortiWeb uses to respond to blocked requests.</p> <p>Valid values are 1 to 600.</p> <p>This option is applicable only if you do not specify a value for error-page.</p>	
health <health-check_name>	<p>Type the name of a server health check to use when determining responsiveness of physical servers in the server farm. The maximum length is 35 characters.</p> <p>To display the list of existing health checks, type:</p> <pre>edit ?</pre> <p>This option is applicable only if <code>deployment-mode</code> is <code>server-balance</code> or <code>content-routing</code>.</p> <p>Note: If a physical server is unresponsive, wait until the server becomes responsive again before disabling its server health check. Server health checks record the up or down status of the server. If you deactivate the server health check while the server is unresponsive, the server health check cannot update the recorded status, and FortiWeb appliance will continue to regard the physical server as if it were unresponsive. You can determine the physical server's connectivity status using the <i>Service Status</i> widget (see the FortiWeb Administration Guide) or an SNMP trap (see “config system snmp community” on page 234).</p>	No default.
intermediate-certificate-group <CA-group_name>	<p>Select the name of an intermediate certificate authority (CA) group, if any, that will be used to validate the CA signing chain in a client's certificate. The maximum length is 35 characters.</p> <p>To display the list of existing groups, type:</p> <pre>edit ?</pre> <p>This option is applicable only if <code>ssl-client-verify</code> is configured and the FortiWeb appliance is operating in reverse proxy mode.</p>	No default.

Variable	Description	Default
lb-algo {round-robin weighted-round-robin least-connection http-session-based-round-robin}	<p>Select one of the following load-balancing algorithms to use when distributing new connections amongst physical servers in the server farm.</p> <ul style="list-style-type: none"> round-robin — Distributes new connections to the next physical server in the server farm, regardless of weight, response time, traffic load, or number of existing connections. Unresponsive servers are avoided. weighted-round-robin — Distributes new connections using the round robin method, except that physical servers with a higher weight value will receive a larger percentage of connections. least-connection — Distributes new connections to the physical server with the fewest number of existing, fully-formed connections. http-session-based-round-robin — Distributes new connections, if they are not associated with an existing HTTP session, to the next physical server in the server farm, regardless of weight, response time, traffic load, or number of existing connections. Unresponsive servers are avoided. This option is available only if type is waf-protection. <p>Note: Session management is not enabled automatically when you enable this feature, and therefore it requires that you enable http-session-management {enable disable} in the web protection profile.</p> <p>This field appears only if deployment-mode is server-balance.</p>	No default.
noparse {enable disable}	<p>Enable this option to apply the server policy as a pure proxy, without parsing the content. In this case, the policy allows all traffic to pass through the FortiWeb appliance without applying any protection rules. See also “debug application http” on page 435 and “debug flow trace” on page 455.</p> <p>This option applies to server policy only when the FortiWeb appliance operates in reverse proxy or true transparent proxy mode.</p> <p>Caution: Use this only during debugging and for as brief a period as possible. This feature disables many protection features. See also config http-parse-error-output {enable disable} in “config config log attack-log” on page 65.</p>	disable
http-pipeline {enable disable}	<p>Enable to accelerate transactions by bundling them inside the same TCP connection, instead of waiting for a response before sending/receiving the next request. This can increase performance when pages containing many images, scripts, and other auxiliary files are all hosted on the same domain, and therefore logically could use the same connection.</p> <p>Only GET and HEAD methods are supported. Clients must include the Connection: keep-alive HTTP header and use HTTP 1.1 (not 1.0) in order to trigger FortiWeb to allow pipelined requests and send pipelined responses.</p> <p>This feature is supported only when FortiWeb is operating in reverse proxy or true transparent proxy mode.</p>	disable

Variable	Description	Default
<code>persistence-timeout</code> <code><timeout_int></code>	Type the timeout for inactive TCP/IP sessions. The valid range is from 0 to 4,294,967,295. This field appears only if <code>deployment-mode</code> is <code>server-balance</code> or <code>transparent-servers</code> .	0
<code>persistent-server-sessions</code> <code><http-sessions_int></code>	Type the maximum number of concurrent TCP client connections that can be accepted by this policy. The valid range is from 1,000 to 10,000. The maximum number of HTTP sessions for each physical server depends on this field, and whether you have selected a single physical server or a server farm, and <code>lb-algo</code> . For example, if the value of <code>persistent-server-sessions</code> is 10,000 and there are 4 physical servers in a server farm that uses round robin-style load-balancing, up to 10,000 client connections would be accepted, resulting in up to 2,500 HTTP sessions evenly distributed to each of the 4 physical servers. For more information, see the maximum values matrix in the FortiWeb Administration Guide . This option appears only if <code>deployment-mode</code> is not <code>offline-detection</code> .	0
<code>pserver</code> <code><pserver_name></code>	Type the name of a single physical server to which to forward connections. The maximum length is 35 characters. To display the list of existing servers, type: <code>edit ?</code> This field is applicable only if <code>deployment-mode</code> is <code>single-server</code> .	No default.
<code>pserver-port</code> <code><port_int></code>	Type the port number on which the HTTP physical server listens for web connections. The valid range is from 1 to 65,535. This field is applicable only if <code>deployment-mode</code> is <code>single-server</code> and <code>service</code> is set.	80
<code>pserver-sport</code> <code><port_int></code>	Type the port number on which the HTTPS physical server listens for web connections. The valid range is from 1 to 65,535. This field is applicable only if <code>https-service</code> is set.	443

Variable	Description	Default
<code>pservers <server-farm_name></code>	<p>Type the name of the server farm whose physical servers will receive the connections. The maximum length is 35 characters.</p> <p>To display the list of existing server farms, type:</p> <pre>edit ?</pre> <p>This option appears only if <code>deployment-mode</code> is <code>server-balance</code>, <code>http-content-routing</code>, <code>offline-detection</code>, or <code>transparent-servers</code>.</p> <p>Note: If <code>deployment-mode</code> is <code>offline-detection</code> or <code>transparent-servers</code>, you must select a server farm, even though the FortiWeb appliance will be allowing connections to pass through instead of actively distributing connections. Therefore if you want to govern connections for only a single physical server, rather than a group of servers, you must configure a server farm with that single physical server as its only member in order to select it in the policy.</p>	No default.
<code>server-connection-pool {enable disable}</code>	<p>Enable this option to improve performance by multiplexing client TCP connections into a single connection to the protected host.</p> <p>Caution: If you enable this option, monitor your FortiWeb appliance closely. This option can cause problems in many network configurations.</p>	disable
<code>service <service_name></code>	<p>Type the custom or predefined service that defines the port number on which the virtual server or bridge receives HTTP traffic. The maximum length is 35 characters.</p> <p>To display the list of existing services, type:</p> <pre>edit ?</pre> <p>This field is applicable only if <code>deployment-mode</code> is not <code>offline-detection</code>.</p>	No default.
<code>https-service <service_name></code>	<p>Type the custom or predefined service that defines the port number on which the virtual server or bridge receives HTTPS traffic. This setting works with <code>pserver-sport</code>. The maximum length is 35 characters.</p> <p>To display the list of existing services, type:</p> <pre>edit ?</pre> <p>This field is applicable only if <code>deployment-mode</code> is not <code>offline-detection</code>.</p>	No default.
<code>hsts-header {enable disable}</code>	<p>Enable to combat MITM attacks on HTTP by injecting the RFC 6797 strict transport security header into the reply, such as:</p> <pre>Strict-Transport-Security: max-age=31536000; includeSubDomains</pre> <p>This forces the client to use HTTPS for subsequent visits to this domain. If the certificate does not validate, it also causes a fatal connection error: the client's web browser will not display any dialog that allows the user to override the certificate mismatch error and continue.</p> <p>This setting applies only if <code>https-service <service_name></code> is configured, and only if the operation mode is reverse proxy.</p>	disable

Variable	Description	Default
hsts-max-age <timeout_int>	<p>Type the time to live in seconds for the HSTS header.</p> <p>This setting applies only if <code>hsts-header {enable disable}</code> is enabled.</p> <p>The valid range is from 3600 to 31,536,000.</p>	7776000

Variable	Description	Default
ssl-client-verify <verifier_name>	<p>Type the name of a certificate verifier, if any, to use when an HTTP client presents their personal certificate. (If you do not select one, the client is not required to present a personal certificate.)</p> <p>If the client presents an invalid certificate, the FortiWeb appliance will not allow the connection.</p> <p>To be valid, a client certificate must:</p> <ul style="list-style-type: none"> • Not be expired • Not be revoked by either the certificate revocation list (CRL) or, if enabled, the online certificate status protocol (OCSP) (see “config system certificate verify” on page 197) • Be signed by a certificate authority (CA) whose certificate you have imported into the FortiWeb appliance (see the FortiWeb Administration Guide); if the certificate has been signed by a chain of intermediate CAs, those certificates must be included in an intermediate CA group (see intermediate-certificate-group <CA-group_name>) • Contain a <code>CA</code> field whose value matches the CA certificate • Contain an <code>Issuer</code> field whose value matches the <code>Subject</code> field in the CA certificate <p>Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the web site.</p> <p>You can require that clients present a certificate alternatively or in addition to HTTP authentication. For more information, see the FortiWeb Administration Guide.</p> <p>The maximum length is 35 characters.</p> <p>To display the list of existing verifiers, type:</p> <pre>edit ?</pre> <p>This option is applicable only if <code>ssl-client</code> is <code>enable</code>, and only applies if the FortiWeb appliance is operating in reverse proxy mode. SSL 3.0 or TLS 1.0 is required.</p> <p>Note: If the connection fails when you have selected a certificate verifier, verify that the certificate meets the web browser’s requirements. Web browsers may have their own certificate validation requirements in addition to FortiWeb requirements. For example, personal certificates for client authentication may be required to either:</p> <ul style="list-style-type: none"> • not be restricted in usage/purpose by the CA, or • contain a <code>Key Usage</code> field that contains <code>Digital Signature</code> or have a <code>ExtendedKeyUsage</code> or <code>EnhancedKeyUsage</code> field whose value contains <code>Client Authentication</code> <p>If the certificate does not satisfy browser requirements, although it may be installed in the browser, when the FortiWeb appliance requests the client’s certificate, the browser may not display a certificate selection dialog to the user, or the dialog may not contain that certificate. In that case, verification will fail. For browser requirements, see your web browser’s documentation.</p>	No default.

Variable	Description	Default
ssl-server {enable disable}	<p>Enable to use SSL/TLS to encrypt connections from the FortiWeb appliance to protected web servers.</p> <p>Disable to pass traffic to protected web servers in clear text.</p> <p>Applies to reverse proxy mode only. (The FortiWeb appliance cannot act as an SSL/TLS terminator or initiator in offline protection mode or transparent inspection mode.)</p> <p>Note: Enable <i>only</i> if the protected host supports HTTPS.</p>	No default.
vserver <vserver_name>	<p>Type the name of a virtual server. The maximum length is 35 characters.</p> <p>To display the list of existing virtual servers, type:</p> <pre>edit ?</pre> <p>Use of this option varies by operating mode:</p> <ul style="list-style-type: none"> Reverse proxy — Select the virtual server to indicate the IP address and network interface of incoming traffic that will be routed and to which the policy will apply a profile. Offline protection — Select the virtual server to indicate the network interface of incoming traffic to which the policy will attempt to apply a profile. The IP address of the virtual server will be ignored. <p>This option appears only if the FortiWeb appliance is operating in reverse proxy or offline protection mode. Otherwise, configure v-zone <bridge_name> instead.</p>	No default.
v-zone <bridge_name>	<p>Select the name of a bridge to whose incoming traffic the policy will apply a profile. The maximum length is 15 characters.</p> <p>To display the list of existing bridges, type:</p> <pre>edit ?</pre> <p>This option appears only if the FortiWeb appliance is operating in true transparent proxy or transparent inspection mode. Otherwise, configure vserver <vserver_name> instead.</p>	No default.
waf-autolearning-profile <profile_name>	<p>Type the auto-learning profile, if any, to use in order to discover attacks, URLs, and parameters in your web servers' HTTP sessions. The maximum length is 35 characters.</p> <p>To display the list of existing profiles, type:</p> <pre>edit ?</pre> <p>Data gathered using an auto-learning profile can be viewed in an auto-learning report, and can be used to generate inline or offline protection profiles. For details, see the FortiWeb Administration Guide.</p> <p>This option appears only if deployment-mode is offline-detection.</p>	No default.

Variable	Description	Default
web-protection-profile <profile_name>	Type the name of the web protection or detection profile to apply to the connections accepted by this policy. The maximum length is 35 characters. To display the list of existing profiles, type: edit ? This field is available only if type is web-protection.	No default.
syncookie {enable disable}	Enable to detect TCP SYN flood attacks (see “config system dos-prevention” on page 203 for additional information). This option applies to server policy only when the FortiWeb appliance operates in true transparent mode.	disable
half-open-threshold <packets_int>	Enter the maximum number of TCP SYN packets, including retransmission, that may be sent per second to a destination address. If this threshold is exceeded, the FortiWeb appliance treats the traffic as a DoS attack and ignores additional traffic from that source address. The valid range is from 10 to 10,000 packets. This option applies to server policy only when the FortiWeb appliance operates in true transparent mode and when syncookie is enabled.	100

Example

This example configures a web protection server policy. HTTPS connections received by the virtual server named `virtual_ip1` are forwarded to a single physical server named `apache1`. The FortiWeb appliance will use the certificate named `certificate1` during SSL negotiations with the client, then forward traffic to the physical server using clear text.

While clients will connect to the virtual server on the FortiWeb appliance using TCP port 443, the standard port number for HTTPS connections, the FortiWeb appliance will actually forward the connections to TCP port 1443, which is the port number on which the physical server listens.

```
config server-policy policy
  edit "https-policy"
    set deployment-mode single-server
    set vserver "virtual_ip1"
    set https-service "HTTPS"
    set web-protection-profile "inline-protection1"
    set pserver "apache1"
    set pserver-sport 1443
    set persistent-server-sessions 1000
    set ssl-server disable
    set certificate "certificate1"
    set case-sensitive disable
    set status enable
  next
end
```


Related topics

- [config server-policy allow-hosts](#)
- [config system certificate local](#)
- [config server-policy health](#)
- [config server-policy pserver](#)
- [config server-policy pservers](#)
- [config server-policy service custom](#)
- [config server-policy vserver](#)
- [config system dos-prevention](#)
- [config system snmp community](#)
- [config system settings](#)
- [config system v-zone](#)
- [config waf web-protection-profile autolearning-profile](#)
- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config server-policy error-page](#)
- [diagnose debug application dssl](#)
- [diagnose debug application http](#)
- [diagnose debug application ssl](#)
- [diagnose debug application ustack](#)
- [diagnose debug flow filter](#)
- [diagnose policy](#)

server-policy pserver

Use this command to configure physical servers.

Physical servers define an individual server or a member of a server farm that is the ultimate destination of traffic received by the FortiWeb appliance at a virtual server address, and to which the FortiWeb appliance will forward traffic after applying the protection profile and other policy settings.

To apply physical servers, select them within a server policy or a server farm that is selected in a policy. For details, see [“config server-policy policy” on page 140](#) or [“config server-policy pserver” on page 154](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pserver
  edit <physical-server_name>
    set status {enable | disable}
    set ip {<server_ipv4> | <server_ipv6>}
  next
end
```

Variable	Description	Default
<physical-server_name>	Type the name of a physical server. The maximum length is 35 characters. To display the list of existing servers, type: <code>edit ?</code>	No default.
status {enable disable}	Enable to forward connections accepted by the policy to the physical server.	enable
ip {<server_ipv4> <server_ipv6>}	Type the IP address of the physical server.	No default.

Example

This example configures a physical server named `soap-server1`.

```
config server-policy pserver
  edit "soap-server1"
    set ip 172.16.1.10
    set status enable
  next
end
```

Related topics

- [config server-policy policy](#)
- [config server-policy pservers](#)
- [config server-policy dserver](#)

server-policy pservers

Use this command to configure server farms.

Server farms define a group of physical servers among which connections will be distributed to or passed through to, depending on the FortiWeb appliance's operating mode (reverse proxy mode actively distributes connections; offline protection and either of the transparent modes do not.)

To apply server farms, select them within a server policy. For details, see [“config server-policy policy” on page 140](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy pservers
edit <server-farm_name>
    set comment "<comment_str>"
    set type {http-content-routing | offline-protection | server-
balance | transparent-servers-for-ti | transparent-servers-for-tp}
    config pserver-list
        edit <entry_index>
            set server-type {physical | domain}
            set pserver <physical-server_name>
            set dserver <domain-server_name>
            set certificate <certificate_name>
            set certificate-verify <verifier_name>
            set client-certificate {enable | disable}
            set http-content-routing-policy <policy_name>
            set intermediate-certificate-group <CA-group_name>
            set port <port_int>
            set ssl {enable | disable}
            set hsts-header {enable | disable}
            set hsts-max-age <timeout_int>
            set weight <weight_int>
        next
    end
next
end
```

Variable	Description	Default
<server-farm_name>	Type the name of the server farm. The maximum length is 35 characters. To display the list of existing servers, type: edit ?	No default.
comment "<comment_str>"	Type a description or other comment. If the comment is more than one word or contains special characters, surround the comment with double quotes ("). The maximum length is 63 characters.	No default.

Variable	Description	Default
type {http-content-routing offline-protection server-balance transparent-servers-for-ti transparent-servers-for-tp}	<p>Select the method of distribution that the FortiWeb appliance will use when forwarding connections to the physical servers in this server farm.</p> <p>For details, see deployment-mode {single-server server-balance http-content-routing offline-detection transparent-servers} in “config server-policy policy” on page 140.</p>	server-balance
<entry_index>	<p>Type the index number of the physical server entry within the server farm. The valid range is from 1 to 9,223,372,036,854,775,807.</p> <p>The first physical server will receive connections if you have configured XPath or WSDL content-based routing and the other server is unavailable. For round robin-style load-balancing, the index number indicates the order in which connections will be distributed.</p> <p>Note: If the server farm will be used with a policy whose deployment-mode is content-routing or wsdl-content-routing, place the physical server that you want to be the failover first in the list of physical servers in the server farm. Because in HTTP header-based routing or WSDL content-based routing each server in the server farm may not host identical web services, if a physical server is unresponsive to the server health check, the FortiWeb appliance will forward subsequent connections to the first physical server in the server farm, which will be considered to be the failover. The first physical server must be able to act as a backup for all of the other servers in the server farm.</p>	No default.
server-type {physical domain}	Select the server type. Depending on this selection, configure either pserver <physical-server_name> or dserver <domain-server_name> .	physical
certificate <certificate_name>	<p>Type the name of the physical server's certificate that the FortiWeb appliance will use when decrypting SSL-secured connections.</p> <p>This setting is applicable only if <code>ssl</code> is <code>enable</code>. The maximum length is 35 characters.</p> <p>To display the list of existing certificates, type:</p> <pre>edit ?</pre>	No default.

Variable	Description	Default
certificate-verify <verifier_name>	<p>Type the name of a certificate verifier, if any, to use when an HTTP client presents their personal certificate. (If you do not select one, the client is not required to present a personal certificate.)</p> <p>Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the web site. For information on how the client's certificate is verified, see ssl-client-verify <verifier_name> in “server-policy policy” on page 140.</p> <p>You can require that clients present a certificate alternatively or in addition to HTTP authentication (see “waf http-authen http-authen-rule” on page 310).</p> <p>This option is available only if <code>ssl</code> is <code>enable</code>, and only applies if the FortiWeb appliance is operating in transparent proxy mode. (For reverse proxy mode, configure this setting in the server policy instead. See ssl-client-verify <verifier_name> in “server-policy policy” on page 140.)</p> <p>The maximum length is 35 characters.</p> <p>To display the list of existing verifiers, type:</p> <pre>edit ?</pre> <p>Note: The client must support SSL 3.0 or TLS 1.0.</p>	No default.
client-certificate {enable disable}	<p>Type the name of a certificate verification rule. The maximum length is 35 characters.</p> <p>Enable to include the X.509 personal certificate presented by the client during the SSL/TLS handshake, if any, in an <code>X-Client-Cert</code>: HTTP header when forwarding the traffic to the protected web server.</p> <p>FortiWeb will still validate the client certificate itself, but this can be useful if the web server requires the client certificate for the purpose of server-side identity-based functionality.</p> <p>This option is available only if <code>ssl</code> is <code>enable</code>, and only applies if the FortiWeb appliance is operating in transparent proxy mode. (For reverse proxy mode, configure this setting in the server policy instead. See client-certificate-forwarding {enable disable} in “server-policy policy” on page 140.)</p> <p>To display the list of existing rules, type:</p> <pre>edit ?</pre>	disable
http-content-routing-policy <policy_name>	<p>Select the HTTP routing policy to route HTTP requests to a specific physical server in a server farm by specifying the host or URL and the request file. The maximum length is 35 characters.</p> <p>To display the list of existing policies, type:</p> <pre>edit ?</pre>	No default.

Variable	Description	Default
intermediate-certificate-group <CA-group_name>	<p>Select the name of a group of intermediate certificate authority (CA) certificates, if any, that will be presented to clients in order to complete the signing chain for them to validate the server certificate's CA signature.</p> <p>If clients receive certificate warnings that the server certificate configured in certificate <certificate_name> has been signed by an intermediary CA, rather than directly by a root CA or other CA currently trusted by the client, configure this option.</p> <p>Alternatively, include the entire signing chain in the server certificate itself before uploading it to the FortiWeb appliance, thereby completing the chain of trust with a CA already known to the client. See the FortiWeb Administration Guide.</p> <p>This option is available only if an <code>ssl</code> is <code>enable</code>, and only applies if the FortiWeb appliance is operating in transparent proxy mode. (For reverse proxy mode, configure this setting in the server policy instead. See intermediate-certificate-group <CA-group_name> in “server-policy policy” on page 140.)</p>	No default.
port <port_int>	Type the port number on which the physical server listens for connections. The valid range is from 1 to 65,535.	80
pserver <physical-server_name>	<p>Type the name of a physical server that will be a member of the server farm. The maximum length is 35 characters.</p> <p>To display the list of existing servers, type:</p> <pre>edit ?</pre> <p>This option appears only when <code>server-type</code> is set to <code>physical</code>.</p>	No default.
dserver <domain-server_name>	<p>Type the name of a domain server that will be a member of the server farm. The maximum length is 35 characters.</p> <p>To display the list of existing servers, type:</p> <pre>edit ?</pre> <p>This option appears only when <code>server-type</code> is set to <code>domain</code>.</p>	No default.

Variable	Description	Default
ssl {enable disable}	<p>Enable if:</p> <ul style="list-style-type: none"> connections to the server use SSL/TLS, and the FortiWeb appliance is operating in a mode other than reverse proxy <p>Also configure certificate <certificate_name>.</p> <p>Unlike https-service <service_name> in policies, when you enable this option, the FortiWeb appliance will not apply SSL. Instead, it will use the certificate to decrypt and scan connections before passing the encrypted traffic through to the web servers or clients (SSL inspection).</p> <p>SSL 3.0, TLS 1.0, and TLS 1.1 are supported.</p> <p>Caution: You must enable either this option in the policy if the connection uses SSL. Failure to enable an SSL option and provide a certificate will result in the FortiWeb appliance being unable to decrypt connections, and therefore unable to scan HTML or XML content.</p> <p>Note: When this option is enabled, the web server must be configured to apply SSL. The FortiWeb appliance will use the certificate to decrypt and scan traffic only. It will not apply SSL to the connections.</p> <p>Note: Ephemeral (temporary key) Diffie-Hellman exchanges are not supported if the FortiWeb appliance is operating in offline protection mode.</p>	No default.
hsts-header {enable disable}	<p>Enable to combat MITM attacks on HTTP by injecting the RFC 6797 strict transport security header into the reply, such as:</p> <pre>Strict-Transport-Security: max-age=31536000; includeSubDomains</pre> <p>This forces the client to use HTTPS for subsequent visits to this domain. If the certificate does not validate, it also causes a fatal connection error: the client's web browser will not display any dialog that allows the user to override the certificate mismatch error and continue.</p> <p>This setting applies only if ssl {enable disable} is enabled, and only if the operation mode is true transparent proxy.</p>	disable
hsts-max-age <timeout_int>	<p>Type the time to live in seconds for the HSTS header.</p> <p>This setting applies only if hsts-header {enable disable} is enabled.</p>	7776000
weight <weight_int>	<p>If the server farm will be used with the weighted round robin load-balancing algorithm, type the numerical weight of the physical server. Physical servers with a greater weight will received a greater proportion of connections.</p> <p>The valid range is from 1 to 9,999.</p>	0

Example

This example configures a server farm named `server-farm1`, which consists of two physical servers: `physical-server1` and `physical-server2`.

When both servers are available, catalog requests matching `content-routing-group1` are forwarded to `physical-server1`; requests matching `content-routing-group2` are forwarded to `physical-server2`. If `physical-server2` is down, all requests are forwarded to `physical-server1`, because it is the first physical server in the server farm.

```
config server-policy pservers
  edit "server-farm1"
    set comment "catalog DB servers in rack 2"
    config pserver-list
      edit 1
        set pserver "physical-server1"
        set ssl disable
        set port 8081
        set httpcontent-routing-policy "content-routing-group1"
      next
      edit 2
        set pserver "physical-server2"
        set ssl disable
        set port 8082
        set httpcontent-routing-policy "content-routing-group2"
      next
    end
  next
end
```

Related topics

- [config server-policy policy](#)
- [config server-policy http-content-routing-policy](#)
- [config system certificate local](#)
- [config server-policy pserver](#)
- [config server-policy dserver](#)
- [config server-policy health](#)

server-policy service custom

Use this command to configure a custom service.

You can add a custom services to a policy to define the protocol and listening port of a virtual server. For details, see [“config server-policy policy” on page 140](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy service custom
  edit <service_name>
    set port <port_int>
    set protocol TCP
  next
end
```

Variable	Description	Default
<service_name>	Type the name of the new or existing custom network service, such as SOAP1. The maximum length is 35 characters. To display the list of existing services, type: edit ?	No default.
port <port_int>	Type the port number on which a virtual server will receive TCP/IP connections for HTTP or HTTPS requests. The valid range is from 1 to 65,535.	No default.

Example

This example configures a service definition named SOAP1.

```
config server-policy custom
  edit "SOAP1"
    set port 8081
    set protocol TCP
  next
end
```

Related topics

- [config server-policy vserver](#)
- [config server-policy policy](#)
- [config server-policy service predefined](#)

server-policy service predefined

Use this command to view a predefined service.



This command only displays predefined services. It **cannot** be used to modify them. If you attempt to edit the port number and protocol, the appliance will discard your settings.

Predefined Internet services can be selected in a policy in order to define the protocol and listening port of a virtual server. For details, see [“config server-policy policy” on page 140](#).

To use this command, your administrator account’s access control profile must have either w or rw permission to the traroutegrp area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy service predefined
  edit <service_name>
    show
  next
end
```

Variable	Description	Default
<service_name>	Type the name of a predefined network service, such as HTTP or HTTPS. The maximum length is 35 characters. To display the list of existing services, type: edit ?	No default.

Example

This example shows the default settings for all of the predefined services.

```
config server-policy service predefined
  show
```

Output:

```
config server-policy service predefined
  edit "HTTP"
    set port 80
    set protocol TCP
  next
  edit "HTTPS"
    set port 443
    set protocol TCP
  next
end
```

Related topics

- [config server-policy vserver](#)
- [config server-policy policy](#)
- [config server-policy service custom](#)

server-policy vserver

Use this command to configure virtual servers.

Before you can create a policy, you must first configure a virtual server which defines the network interface or bridge and IP address on which traffic destined for an individual physical server or server farm will arrive.

When the FortiWeb appliance receives traffic destined for a virtual server, it can then forward the traffic to a physical server or a server farm. The FortiWeb appliance identifies traffic as being destined for a specific virtual server if:

- the traffic arrives on the network interface or bridge associated with the virtual server
- for reverse proxy mode, the destination address is the IP address of a virtual server (the destination IP address is ignored in other operation modes, **except** that it must **not** be identical with the physical server's IP address)



Virtual servers can be on the same subnet as physical servers. This configuration creates a one-arm HTTP proxy. For example, the virtual server 10.0.0.1/24 could forward to the physical server 10.0.0.2.

However, this is **not** recommended. Unless your network's routing configuration prevents it, it could allow attackers that are aware of the physical server's IP address to bypass FortiWeb by accessing the physical server directly.

To apply virtual servers, select them within a server policy. For details, see [“config server-policy policy” on page 140](#).

To use this command, your administrator account's access control profile must have either w or rw permission to the traroutegrp area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config server-policy vserver
  edit <virtual-server_name>
    set status {enable | disable}
    set interface <interface_name>
    set vip <virtual-ip_ipv4mask>
    [set vip6 <virtual-ip_ipv6mask>]
  next
end
```

Variable	Description	Default
<virtual-server_name>	Type the name of the new or existing virtual server. The maximum length is 35 characters. To display the list of existing servers, type: edit ?	disable
status {enable disable}	Enable to accept traffic destined for this virtual server.	No default.

Variable	Description	Default
interface <interface_name>	Type the name of the network interface or bridge, such as <code>port1</code> or <code>bridge1</code> , to which the virtual server is bound, and on which traffic destined for the virtual server will arrive. The maximum length is 35 characters. To display the list of existing interfaces, type: <code>edit ?</code>	No default.
vip <virtual-ip_ipv4mask>	Type the IPv4 address and subnet of the virtual server.	0.0.0.0 0.0.0.0
vip6 <virtual-ip_ipv6mask>	Type the IPv6 address and subnet of the virtual server.	::/0

Example

This example configures a virtual server named `inline_vip1` on the network interface named `port1`.

The port number on which the virtual server will receive traffic is defined separately, in the policies that use this virtual server definition.

```
config server-policy vserver
  edit "inline_vip1"
    set status enable
    set interface port1
    set vip 10.0.0.1 255.255.255.0
  next
end
```

Related topics

- [config system interface](#)
- [config server-policy policy](#)
- [config server-policy service custom](#)
- [execute ping](#)
- [diagnose network ip](#)

system accprofile

Use this command to configure access control profiles for administrators.



If you have configured RADIUS queries for authenticating administrators, you can override the locally-selected access profile by using a RADIUS VSA. See [“config system admin” on page 170](#).

Access profiles determine administrator accounts' permissions.

When an administrator has only read access to a feature, the administrator can access the web UI page for that feature, and can use the `get` and `show` CLI command for that feature, but cannot make changes to the configuration. There are no *Create* or *Apply* buttons, or `config` CLI commands. Lists display only the *View* icon instead of icons for *Edit*, *Delete* or other modification commands. Write access is required for modification of any kind.

In larger companies where multiple administrators divide the share of work, access profiles often reflect the specific job that each administrator does (“role”), such as user account creation or log auditing. Access profiles can limit each administrator account to their assigned role. This is sometimes called role-based access control (RBAC).

The `prof_admin` access profile, a special access profile assigned to the `admin` administrator account and required by it, **does not** appear in the list of access profiles. It exists by default and cannot be changed or deleted, and consists of essentially UNIX `root`-like permissions.



Even if you assign the `prof_admin` access profile to other administrators, they will **not** have all of the same permissions as the `admin` account. The `admin` account has some special permissions, such as the ability to reset administrator passwords, that are inherent in that account only. Other accounts should not be considered a complete substitute.

If you create more administrator accounts, whether to harden security or simply to prevent accidental modification, create other access profiles with the minimal degrees and areas of access that each role requires. Then assign each administrator account the appropriate role-based access profile.

For example, for a person whose only role is to audit the log messages, you might make an access profile named `auditor` that only has *Read* permissions to the *Log & Report* area.

For information on how each access control area correlates to which CLI commands that administrators can access, see [“Permissions” on page 47](#)

To use this command, your administrator account's access control profile must have both `r` and `w` permissions to items in the `admingrp` category.

Syntax

```
config system accprofile
edit <access-profile_name>
    set admingrp {none | r | rw | w}
    set authusergrp {none | r | rw | w}
    set learngrp {none | r | rw | w}
    set loggrp {none | r | rw | w}
    set mntgrp {none | r | rw | w}
    set netgrp {none | r | rw | w}
```

```

set sysgrp {none | r | rw | w}
set traroutegrp {none | r | rw | w}
set wadgrp {none | r | rw | w}
set webgrp {none | r | rw | w}
set wvsgrp {none | r | rw | w}

next
end

```

Variable	Description	Default
<access-profile_name>	Type the name of the access profile. The maximum length is 35 characters. To display the list of existing profiles, type: edit ?	No default.
admingrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the system administrator configuration. Available only when administrative domains (ADOMs) are disabled. See adom-admin {enable disable} in “config system global” on page 206.	none
authusergrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the HTTP authentication user configuration.	none
learngrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the auto-learning profiles and their resulting auto-learning reports.	none
loggrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the logging and alert email configuration.	none
mntgrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to maintenance commands. Unlike the other rows, whose scope is an area of the configuration, the maintenance access control area does not affect the configuration. Instead, it indicates whether the administrator can perform special system operations such as changing the firmware.	none
netgrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the network interface and routing configuration.	none
sysgrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the basic system configuration (except for areas included in other access control areas such as admingrp).	none
traroutegrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the server policy (formerly called traffic routing) configuration.	none
wadgrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the web anti-defacement configuration.	none

Variable	Description	Default
webgrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the web protection profile configuration.	none
wvsgrp {none r rw w}	Type the degree of access that administrator accounts using this access profile will have to the web vulnerability scanner.	none

Example

This example configures an administrator access profile named `full_access`, which permits both read and write access to all special operations and parts of the configuration.



Even though this access profile configures full access, administrator accounts using this access profile will **not** be fully equivalent to the `admin` administrator. The `admin` administrator has some special privileges that are inherent in that account and cannot be granted through an access profile, such as the ability to reset other administrators' passwords without knowing their current password. Other accounts should therefore not be considered a substitute, even if they are granted full access.

```
config system accprofile
  edit "full_access"
    set admingrp rw
    set authusergrp rw
    set learngrp rw
    set loggrp rw
    set mntgrp rw
    set netgrp rw
    set sysgrp rw
    set traroutegrp rw
    set wadgrp rw
    set webgrp rw
    set wvsgrp rw
  next
end
```

Related topics

- [config system admin](#)
- [config user radius-user](#)
- [Permissions](#)

system admin

Use this command to configure FortiWeb administrator accounts. In its factory default configuration, a FortiWeb appliance has one administrator account, named `admin`. That administrator has permissions that grant full access to the FortiWeb configuration and firmware. After connecting to the web UI or the CLI using the `admin` administrator account, you can configure additional administrator accounts with various levels of access to different parts of the FortiWeb configuration.

Administrators can access the web UI and the CLI through the network, depending on administrator account's trusted hosts, ADOMs, and the administrative access protocols enabled for each of the FortiWeb appliance's network interfaces. For details, see [“config system interface” on page 220](#), [“config system global” on page 206](#), and [“Connecting to the CLI” on page 34](#).

To see which administrators are logged in, use the CLI command [get system logged-users](#).



To prevent multiple administrators from logging in simultaneously, which could allow them to inadvertently overwrite each other's changes, enable `single-admin-mode {enable | disable}`. For details, see [“config system global” on page 206](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system admin
  edit <administrator_name>
    set accprofile <access-profile_name>
    set accprofile-override {enable | disable}
    set domains <adom_name>
    set password <password_str>
    set email-address <contact_email>
    set first-name <name_str>
    set last-name <surname_str>
    set mobile-number <cell-phone_str>
    set phone-number <phone_str>
    set trusthost1 <management-computer_ipv4mask>
    set trusthost2 <management-computer_ipv4mask>
    set trusthost3 <management-computer_ipv4mask>
    set ip6trusthost1 <management-computer_ipv6mask>
    set ip6trusthost2 <management-computer_ipv6mask>
    set ip6trusthost3 <management-computer_ipv6mask>
    set type {local-user | remote-user}
    set admin-usergroup <remote-auth-group_name>
```

```

        set wildcard {enable | disable}
    next
end

```

Variable	Description	Default
<administrator_name>	<p>Type the name of the administrator account, such as admin1 or admin@example.com, that can be referenced in other parts of the configuration.</p> <p>Do not use spaces or special characters except the ‘at’ symbol (@). The maximum length is 35 characters.</p> <p>To display the list of existing accounts, type:</p> <pre>edit ?</pre> <p>Note: This is the user name that the administrator must provide when logging in to the CLI or web UI. If using an external authentication server such as RADIUS or Active Directory, this name will be passed to the server via the remote authentication query.</p>	No default.
accprofile <access-profile_name>	<p>Type the name of an access profile that gives the permissions for this administrator account. See also “config system accprofile” on page 167. The maximum length is 35 characters.</p> <p>You can select <i>prof_admin</i>, a special access profile used by the admin administrator account. However, selecting this access profile will not confer all of the same permissions of the admin administrator. For example, the new administrator would not be able to reset lost administrator passwords.</p> <p>To display the list of existing profiles, type:</p> <pre>edit ?</pre> <p>Tip: Alternatively, if your administrator accounts authenticate via a RADIUS query, you can assign their access profile through the RADIUS server using RFC 2548 Microsoft Vendor-specific RADIUS Attributes.</p> <p>On the RADIUS server, create an attribute named:</p> <pre>ATTRIBUTE FortiWeb-Access-Profile 7</pre> <p>then set its value to be the name of the access profile that you want to assign to this account. Finally, in the CLI, use accprofile-override {enable disable} to enable the override.</p> <p>If none is assigned on the RADIUS server, or if it does not match the name of an existing access profile on FortiWeb, FortiWeb will fail back to use the one locally assigned by this setting.</p>	No default.
accprofile-override {enable disable}	<p>Enable to use the access profile indicated by the RADIUS query response, and ignore accprofile <access-profile_name>.</p> <p>This setting applies only if admin-usergroup <remote-auth-group_name> is configured to use a RADIUS query to authenticate this account.</p> <p>This setting applies only if ADOMs are enabled. See adom-admin {enable disable} in “config system global” on page 206.</p>	disable

Variable	Description	Default
domains <adom_name>	Type the name of an administrative domain (ADOM) to assign and restrict this administrative account to it. This setting applies only if ADOMs are enabled. See adom-admin {enable disable} in “config system global” on page 206.	No default.
password <password_str>	Type a password for the administrator account. The maximum length is 32 characters. The minimum length is 1 character. For improved security, the password should be at least 8 characters long, be sufficiently complex, and be changed regularly. This setting applies only when type is local-user. For accounts defined on a remote authentication server, the FortiWeb appliance will instead query the server to verify whether the password given during a login attempt matches the account’s definition.	No default.
email-address <contact_email>	Type an email address that can be used to contact this administrator. The maximum length is 35 characters.	No default.
first-name <name_str>	Type the first name of the administrator. The maximum length is 35 characters.	No default.
last-name <surname_str>	Type the surname of the administrator. The maximum length is 35 characters.	No default.
mobile-number <cell-phone_str>	Type a cell phone number that can be used to contact this administrator. The maximum length is 35 characters.	No default.
phone-number <phone_str>	Type a phone number that can be used to contact this administrator. The maximum length is 35 characters.	No default.
trusthost1 <management-computer_ipv4mask>	Type the IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. You can specify up to three trusted hosts. To allow login attempts from any IP address, enter 0.0.0.0/0.0.0.0. If you allow logins from any IP address, consider choosing a longer and more complex password, and limiting administrative access to secure protocols to minimize the security risk. For information on administrative access protocols, see “config system interface” on page 220. Note: For improved security, restrict all three trusted host addresses to the IP addresses of computers from which only this administrator will log in.	0.0.0.0 0.0.0.0
trusthost2 <management-computer_ipv4mask>	Type a second IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. To allow login attempts from any IP address, enter 0.0.0.0/0.0.0.0.	0.0.0.0 0.0.0.0
trusthost3 <management-computer_ipv4mask>	Type a third IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. To allow login attempts from any IP address, enter 0.0.0.0/0.0.0.0.	0.0.0.0 0.0.0.0

Variable	Description	Default
ip6trusthost1 <management-computer_ipv6mask>	<p>Type the IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. You can specify up to three trusted hosts.</p> <p>To allow login attempts from any IP address, enter <code>::/0</code>.</p> <p>Caution: If you allow logins from any IP address, consider choosing a longer and more complex password, and limiting administrative access to secure protocols to minimize the security risk. Unlike IPv4, IPv6 does not isolate public from private networks via NAT, and therefore can increase availability of your FortiWeb's web UI/CLI to IPv6 attackers unless you have carefully configured your firewall/FortiGate and routers. For information on administrative access protocols, see “config system interface” on page 220.</p> <p>Note: For improved security, restrict all three trusted host addresses to the IP addresses of computers from which only this administrator will log in.</p>	::/0
ip6trusthost2 <management-computer_ipv6mask>	<p>Type a second IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance.</p> <p>To allow login attempts from any IP address, enter <code>::/0</code>.</p>	::/0
ip6trusthost3 <management-computer_ipv6mask>	<p>Type a third IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance.</p> <p>To allow login attempts from any IP address, enter <code>::/0</code>.</p>	::/0
type {local-user remote-user}	<p>Select either:</p> <ul style="list-style-type: none"> <code>local-user</code> — Authenticate this account locally, with the FortiWeb appliance itself. <code>remote-user</code> — Authenticate this account via a remote server such as an LDAP or RADIUS server. Also configure admin-usergroup <remote-auth-group_name>. 	No default.
admin-usergroup <remote-auth-group_name>	<p>Type the name of the remote authentication group whose settings the FortiWeb appliance will use to connect to a remote authentication server when authenticating login attempts for this account. The maximum length is 35 characters.</p> <p>To display the list of existing groups, type:</p> <pre>edit ?</pre> <p>For details on configuring remote authentication groups, see “config user admin-usergrp” on page 243.</p>	No default.
wildcard {enable disable}	<p>Used when administrator accounts authenticate via a RADIUS query.</p> <p>This setting applies only if the value of <code>type</code> is <code>remote-user</code>.</p>	No default.

Example

This example configures an administrator account with an access profile that grants only permission to read logs. This account can log in only from an IP address on the management LAN (172.16.2.0/24), or from one of two specific IP addresses (172.16.3.15 and 192.168.1.50).

```
config system admin
    edit "log-auditor"
        set accprofile "log_read_access"
        set password P@ssw0rd
        set email-address log-admin@example.com
        set trusthost1 172.16.2.0 255.255.255.0
        set trusthost2 172.16.3.15 255.255.255.255
        set trusthost3 192.168.1.50 255.255.255.255
    next
end
```



To display all dashboard status and widget settings, enter:

```
config system admin
show
```

Related topics

- [config system accprofile](#)
- [config system global](#)
- [config user admin-usergrp](#)

system advanced

Use this command to configure several system-wide options that determine how FortiWeb scans traffic.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system advanced
    set circulate-url-decode {enable | disable}
    set disable-client-side-ssl-negotiations {enable | disable}
    set max-cache-size <cache_int>
    set max-dlp-cache-size <percentage_int>
    set max-dos-alert-interval <seconds_int>
    set max-http-argbuf-length {8k-cache | 12k-cache | 32k-cache | 64k-cache}
    set max-http-header-length {8k-cache | 12k-cache}
    set no-ssl3 {enable | disable}
    set prioritize-rc4-cipher-suite {enable | disable}
    set share-ip {enable | disable}
    set upfile-count {8 | 16}
end
```

Variable	Description	Default
circulate-url-decode {enable disable}	<p>Enable to detect URL-embedded attacks that are obfuscated using recursive URL encoding (that is, multiple levels' worth of URL encoding).</p> <p>Encoded URLs can be legitimately used for non-English URLs, but can also be used to avoid detection of attacks that use special characters. Encoded URLs can now be decoded to scan for these types of attacks. Several encoding types are supported.</p> <p>For example, you could detect the character <code>A</code> that is encoded as either <code>%41</code>, <code>%x41</code>, <code>%u0041</code>, or <code>\t41</code>.</p> <p>Disable to decode only one level's worth of the URL, if encoded.</p>	disable
disable-client-side-ssl-negotiations {enable disable}	<p>Enable to prevent client-initiated SSL/TLS re-negotiation.</p> <p>According to RFC 5246, either the client or the server can re-negotiate the connection in order to change cryptographic keys and other parameters. However, SSL/TLS renegotiation attacks exist to take advantage of the fact that the negotiation phase is more processing-intensive for the server than it is for the client. By repeatedly initiating renegotiations, clients can cause a DoS.</p>	enable
max-cache-size <cache_int>	<p>Type the maximum size in kilobytes (KB) of the body of the HTTP response from the web server that FortiWeb will cache per URL.</p> <p>Responses are cached to improve performance on compression, decompression, and rewriting on often-requested URLs.</p> <p>Valid values range from 32 to 1,024. The default value is 64.</p> <p>Increasing the body cache may decrease performance.</p>	64

Variable	Description	Default
max-dlp-cache-size <percentage_int>	Type the maximum percentage of <code>max-cache-size <cache_int></code> – the body of the HTTP response from the web server – that FortiWeb will buffer and scan. Responses are cached to improve performance on compression, decompression, and rewriting on often-requested URLs.	12
max-dos-alert-interval <seconds_int>	Type the maximum amount of time that FortiWeb will converge into a single log message during a DoS attack or padding oracle attack.	180
max-http-argbuf-length {8k-cache 12k-cache 32k-cache 64k-cache}	Select the maximum buffer size in kilobytes (KB) for each parameter in the HTTP request. The buffer applies regardless of HTTP method, and whether the parameters are in the URL or body. Caution: Fortinet strongly recommends that you configure FortiWeb to block requests larger than this buffer. Parameters exceeding this buffer size cannot be scanned. As a result, unless you configure FortiWeb to block oversized parameters using <code>max-url-parameter-length {enable disable}</code> and <code>max-url-parameter {enable disable}</code> , they will be passed. This could allow oversized attacks to pass through. Some web applications require very large requests or parameters, and will not work if oversized parameters are blocked. To be sure that hardening the configuration will not disrupt normal traffic, first configure <code><parameter_name>-action {alert alert_deny block-period}</code> to be alert. If no problems occur, switch it to <code>alert_deny</code> . Tip: Increasing the buffer size increases memory consumption slightly, and may decrease performance. Only increase this value if necessary.	8k-cache
max-http-header-length {8k-cache 12k-cache}	Select the maximum buffer size in kilobytes (KB) for the Cookie:, User-Agent:, Host:, Referer:, and other headers in the HTTP request. Caution: Fortinet strongly recommends that you configure FortiWeb to block requests if those headers are larger than this buffer. Headers exceeding this buffer size cannot be scanned. As a result, unless you configure FortiWeb to block oversized headers using <code>max-http-header-line-length <limit_int></code> , they will be passed. This could allow oversized attacks to pass through. Some web applications require very large requests, cookies, or parameters, and will not work if oversized parameters or cookies are blocked. To be sure that hardening the configuration will not disrupt normal traffic, first configure <code><parameter_name>-action {alert alert_deny block-period}</code> to be alert. If no problems occur, switch it to <code>alert_deny</code> . Tip: Increasing the buffer size increases memory consumption slightly, and may decrease performance. Only increase this value if necessary.	8k-cache
no-sslsv3 {enable disable}	Enable to prevent clients from connecting to back-end servers via SSL 3.0. Protects against a POODLE (Padding Oracle On Downgraded Legacy Encryption) attack. To disable SSL 3.0 support for web UI access, use <code>config system global</code> .	disable

Variable	Description	Default
<code>prioritize-rc4-cipher-suite {enable disable}</code>	<p>Enable to prefer the RC4 encryption algorithm during cipher negotiation, if the client's hello during the handshake advertises support for it.</p> <p>In older TLS 1.0 implementations, including the NSS cryptographic package used by Mozilla Firefox and Google Chrome web browsers, both AES and 3DES are vulnerable to initialization vector (IV)-based CBC attacks due to using the same IV repeatedly. This causes the cipher blocks to become predictable, and therefore vulnerable to a MITM eavesdropper.</p> <p>Because RC4 is a stream cipher, which does not use CBC, it is not vulnerable to the BEAST attack.</p> <p>Note: This option takes affect only if FortiWeb is operating in reverse proxy or true transparent proxy mode.</p> <p>Caution: Known attacks also exist for RC4, depending on the implementation. Weigh the risks and benefits carefully. You should never use a cipher that is weaker than the value of the data that it is protecting. For information on cipher suites supported by FortiWeb, see the FortiWeb Administration Guide.</p>	enable
<code>share-ip {enable disable}</code>	<p>Enable to analyze the ID field of IP headers in order to attempt to detect when multiple clients share the same source IP address. To configure the difference between packets' ID fields that FortiWeb will treat as a shared IP, use config system ip-detection.</p> <p>Enabling this option is required for features that have a separate threshold for shared IP addresses, such as brute force login prevention. If you disable the option, those features will behave as if there is only a single threshold, regardless of whether the source IP is shared by many clients.</p>	disable
<code>upfile-count {8 16}</code>	Select the maximum number of uploaded files that FortiWeb antivirus will scan before deciding to pass or block the request.	8

Example

This example hardens the configuration against BEAST eavesdropping attacks and SSL/TLS renegotiation DoS attacks.

```
config system advanced
    set prioritize-rc4-cipher-suite enable
    set disable-client-side-ssl-negotiations enable
end
```

Related topics

- [config server-policy policy](#)
- [config system certificate local](#)
- [config system global](#)
- [config system ip-detection](#)
- [config waf brute-force-login](#)
- [config waf application-layer-dos-prevention](#)
- [config waf http-protocol-parameter-restriction](#)

system antivirus

Use this command to configure system-wide FortiGuard Antivirus scan settings.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system antivirus
  set default-db {basic | extended}
  set scan-bzip2 {enable | disable}
  set uncomp-size-limit <limit_int>
  set uncomp-nest-limit <limit_int>
end
```

Variable	Description	Default
default-db {basic extended}	Select which of the antivirus signature databases to use when scanning HTTP POST requests for trojans, either: <ul style="list-style-type: none"><code>basic</code> — Select to use only the signatures of viruses and greyware that have been detected by FortiGuard's networks to be recently spreading in the wild.<code>extended</code> — Select to use all signatures, regardless of whether the viruses or greyware are currently spreading.	basic
scan-bzip2 {enable disable}	Enable to scan archives that are compressed using the BZIP2 algorithm. Tip: Scanning BZIP2 archives can be very CPU-intensive. To improve performance, block the BZIP2 file type, then disable this option.	enable
uncomp-size-limit <limit_int>	Type the maximum size in kilobytes (KB) of the memory buffer that FortiWeb will use to temporarily undo the compression that a client or web server has applied to traffic, in order to inspect and/or modify it. See “waf file-uncompress-rule” on page 290 . Caution: Unless you configure otherwise, compressed requests that are too large for this buffer will pass through FortiWeb without scanning or rewriting. This could allow malware to reach your web servers, and cause HTTP body rewriting to fail. If you prefer to block requests greater than this buffer size, configure max-http-body-length <limit_int> . To be sure that it will not disrupt normal traffic, first configure action to be alert. If no problems occur, switch it to alert_deny.	5000
uncomp-nest-limit <limit_int>	Type the maximum number of allowed levels of compression (“nesting”) that FortiWeb will attempt to decompress.	12

Related topics

- [config system global](#)

system autoupdate override

Use this command to override the default FortiGuard Distribution Server (FDS).

If you cannot connect to the FortiGuard Distribution Network (FDN) or if your organization provides updates using their own FortiGuard server, you can override the FDS server setting so that the FortiWeb appliance connects to this server instead of the default server on Fortinet's public FDN.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system autoupdate override
    set status {enable | disable}
    set address {<fds_fqdn> | <fds_ipv4>}
    set fail-over {enable | disable}
end
```

Variable	Description	Default
status {enable disable}	Enable to override the default list of FDN servers, and connect to a specific server.	disable
address {<fds_fqdn> <fds_ipv4>}	Type either the IP address or fully qualified domain name (FQDN) of the FDS override.	No default.
fail-over {enable disable}	Enable to fail over to one of the public FDN servers if FortiWeb cannot reach the server specified in your FDS override.	enable

Related topics

- [config system autoupdate schedule](#)

system autoupdate schedule

Use this command to configure how the FortiWeb appliance will access the Fortinet Distribution Network (FDN) to retrieve updates. The FDN is a world-wide network that delivers FortiGuard service updates of predefined robots, data types, suspicious URLs, IP address reputations, and attack signatures used to detect attacks such as:

- cross-site scripting (XSS)
- SQL injection
- common exploits



Alternatively, you can manually upload update packages. For details, see the [FortiWeb Administration Guide](#).

FortiWeb appliances connect to the FDN by connecting to the Fortinet Distribution Server (FDS) nearest to the FortiWeb appliance based on its configured time zone.

In addition to manual update requests, FortiWeb appliances support an automatic scheduled updates, by which the FortiWeb appliance periodically polls the FDN to determine if there are any available updates.

If you want to connect to a specific FDS, you must configure [config system autoupdate override](#). If your FortiWeb appliance must connect through a web proxy, you must also configure [config system autoupdate tunneling](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config system autoupdate schedule
    set status {enable | disable}
    set frequency {daily | every | weekly}
    set time <time_str>
    set day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday |
    Saturday}
end
```

Variable	Description	Default
status {enable disable}	Enable to periodically request signature updates from the FDN.	disable
frequency {daily every weekly}	Select the frequency with which the FortiWeb appliance will request signature updates.	every

Variable	Description	Default
time <time_str>	Type the time at which the FortiWeb appliance will request signature updates. The time format is hh:mm, where: <ul style="list-style-type: none"> hh is the hour according to a 24-hour clock mm is the minute 	00:00
day {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}	Select which day of the week that the FortiWeb appliance will request signature updates. This option applies only if frequency is weekly.	Monday

Example

This example configures weekly signature update requests on Sunday at 2:00 PM.

```
config system autoupdate schedule
    set status enable
    set frequency weekly
    set day Sunday
    set time 14:00
end
```

Related topics

- [config system autoupdate override](#)
- [config system autoupdate tunneling](#)
- [config system global](#)

system autoupdate tunneling

Use this command to configure the FortiWeb appliance to use a proxy server to connect to the Fortinet Distribution Network (FDN).

The FortiWeb appliance will connect to the proxy using the HTTP `CONNECT` method, as described in [RFC 2616](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config system autoupdate tunneling
  set status {enable | disable}
  set address {<proxy_fqdn> | <proxy_ipv4>}
  set port <port_int>
  set username <proxy-user_str>
  set password <proxy-password_str>
end
```

Variable	Description	Default
status {enable disable}	Enable to connect to the FDN through a web proxy.	disable
address {<proxy_fqdn> <proxy_ipv4>}	Type either the IP address or fully qualified domain name (FQDN) of the web proxy. The maximum length is 63 characters.	No default.
port <port_int>	Type the port number on which the web proxy listens for connections. The valid range is from 0 to 65,535.	0
username <proxy-user_str>	If the proxy requires authentication, type the FortiWeb appliance's login name on the web proxy. The maximum length is 49 characters.	No default.
password <proxy-password_str>	If the proxy requires authentication, type the password for the FortiWeb appliance's login name on the web proxy. The maximum length is 49 characters.	No default.

Example

This example configures the FortiWeb appliance to connect through a web proxy that requires authentication.

```
config system autoupdate tunneling
  set status enable
  set address 192.168.1.10
  set port 1443
  set username fortibweb
  set password myPassword1
end
```

Related topics

- [config system autoupdate schedule](#)

system backup

Use this command to configure automatic backups of the system configuration to an FTP or SFTP server. You can either run the backup immediately or schedule it to run periodically.

The backup can include all uploaded files such as error pages, WSDL files, certificates, and private keys. Fortinet recommends that if you have many such files, that you include them in the backup. This saves you valuable time if you need to restore the configuration in an emergency.



Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location. This backup method includes sensitive data such as your HTTPS certificates' private keys. Unauthorized access to private keys compromises the security of all HTTPS requests using those certificates.

To restore a backup, see [“execute backup full-config” on page 510](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system backup
edit <backup_name>
    set config-type {full-config | cli-config | waf-config}
    set encryption {enable | disable}
    set encryption-passwd <password_str>
    set ftp-auth {enable | disable}
    set ftp-user <user_str>
    set ftp-passwd <password_str>
    set ftp-dir "<directory-path_str>"
    set ftp-server {<server_ipv4> | <server_fqdn>}
    set protocol-type {ftp | sftp}
    set schedule_type {now | days}
    set schedule_days {sun mon tue wed thu fri sat}
```

```

    set schedule_time <time_str>
next
end

```

Variable	Description	Default
<backup_name>	Type the name of the backup configuration. The maximum length is 59 characters. To display the list of existing backups, type: edit ?	No default.
config-type {full-config cli-config waf-config}	Select either: <ul style="list-style-type: none"> full-config — Include both the configuration file and other uploaded files, such a certificate and error page files, in the backup. cli-config — Include only the configuration file in the backup. waf-config — Include only the web protection profiles in the backup. 	cli-config
encryption {enable disable}	Enable to encrypt the backup file using 128-bit AES and a password. Caution: Unlike when downloading a backup from the web UI to your computer, this does include all certificates and private keys. Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location.	disable
encryption-passwd <password_str>	Type the password that will be used to encrypt the backup file. This field appears only if you enable encryption {enable disable} .	
ftp-auth {enable disable}	Enable if the server requires that you provide a user name and password for authentication, rather than allowing anonymous connections. When enabled, you must also configure ftp-user <user_str> and ftp-passwd <password_str> . Disable for FTP servers that allow anonymous uploads.	disable
ftp-user <user_str>	Type the user name that the FortiWeb appliance will use to authenticate with the server. The maximum length is 127 characters. This variable is not available unless ftp-auth is enable.	No default.
ftp-passwd <password_str>	Type the password corresponding to the account specified in ftp-user <user_str> . The maximum length is 127 characters. This variable is not available unless ftp-auth is enable.	No default.
ftp-dir "<directory-path_str>"	Type the directory path on the server where you want to store the backup file. The maximum length is 127 characters.	No default.

Variable	Description	Default
ftp-server {<server_ipv4> <server_fqdn>}	Type either the IP address or fully qualified domain name (FQDN) of the server. The maximum length is 127 characters.	No default.
protocol-type {ftp sftp}	Select whether to connect to the server using FTP or SFTP.	ftp
schedule_type {now days}	Select one of the schedule types: <ul style="list-style-type: none"> now — Use this to initiate the FTP backup immediately upon ending the command sequence. days — Enter this to allow you to set days and a time to run the backup automatically. You must also configure <code>schedule_days</code> and <code>schedule_time</code>. 	now
schedule_days {sun mon tue wed thu fri sat}	Select one or more days of the week when you want to run a periodic backup. Separate each day with a blank space. For example, to back up the configuration on Monday and Friday, type: set schedule_days mon,fri This command is available only if <code>schedule_type</code> is days.	No default.
schedule_time <time_str>	Type the time of day to run the backup. The time format is hh:mm, where: <ul style="list-style-type: none"> hh is the hour according to a 24-hour clock mm is the minute This command is available only if <code>schedule_type</code> is days.	00:00

Example

This example configures a scheduled, full configuration backup every Sunday and Friday at 1:15 AM. The FortiWeb appliance authenticates with the FTP server using an account named `fortiweb1` and its password, `P@ssword1`. It does not encrypt the backup file.

```
config system backup
    edit "Scheduled_Backup"
        set config-type full-config
        set protocol-type ftp
        set ftp-auth enable
        set ftp-user fortiweb1
        set ftp-passwd P@ssword1
        set ftp-server 172.20.120.01
        set ftp-dir "/config-backups"
        set schedule_type days
        set schedule_days sun,fri
```

```
        set schedule_time 01:15
    next
end
```

Related topics

- [execute restore config](#)
- [execute backup cli-config](#)

system certificate ca

Use this command to edit the comment associated with a certificate for a certificate authority (CA).

Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates are authentic and can be trusted

CA certificates are not used directly, but must first be grouped in order to be selected in a certificate verification rule. For details, see [“config system certificate ca-group” on page 190](#).

For information on how to upload a certificate file, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system certificate ca
  edit <certificate_name>
    set comment "<comment_str>"
  next
end
```

Variable	Description	Default
<certificate_name>	Type the name of a CA certificate file. The maximum length is 35 characters.	No default.
comment "<comment_str>"	Type a description or comment. If the comment is more than one word or contains an apostrophe, surround the words with double quotes ("). The maximum length is 127 characters.	No default.

Related topics

- [config system certificate ca-group](#)
- [config system certificate verify](#)

system certificate ca-group

Use this command to group certificate authorities (CA).

CAs must belong to a group in order to be selected in a certificate verification rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system certificate ca-group
  edit <ca-group_name>
    config members
      edit <ca_index>
        set name <ca_name>
      next
    end
  next
end
```

Variable	Description	Default
<ca-group_name>	Type the name of a certificate authority (CA) group. The maximum length is 35 characters.	No default.
<ca_index>	Type the index number of a CA within its group. The valid range is from 1 to 9,999,999,999,999,999.	No default.
name <ca_name>	Type the name of a previously uploaded CA certificate. The maximum length is 35 characters.	No default.

Example

This example groups two CA certificates into a CA group named `caVendors1`.

```
config system certificate ca-group
  edit "caVendors1"
    config members
      edit 1
        set name "CA_Cert_1"
      next
      edit 2
        set name "CA_Cert_2"
      next
    end
  next
end
```

Related topics

- [config system certificate local](#)
- [config system certificate verify](#)

system certificate crl

Use this command to edit the comment or URL associated with a previously uploaded certificate revocation list (CRL).

To ensure that your FortiWeb appliance validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use HTTP or online certificate status protocol (OCSP) to query for certificate status. For more information, see [“config system certificate remote” on page 196](#).

For information on how to upload a CRL, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system certificate crl
  edit <crl_name>
    set comment "<comment_str>"
    set url <crl_str>
  next
end
```

Variable	Description	Default
<crl_name>	Type the name of a CRL. The maximum length is 35 characters.	No default.
comment "<comment_str>"	Type a description or other comment. If the comment is more than one word or contains an apostrophe, surround the comment with double quotes ("). The maximum length is 127 characters.	No default.
url <crl_str>	If you did not upload a CRL file, but instead will query for it from an HTTP or OCSP server, enter the URL of the CRL. The maximum length is 127 characters.	No default.

Related topics

- [config system certificate local](#)
- [config system certificate verify](#)

system certificate intermediate-certificate

Use this command to edit the comment associated with an intermediate CA certificate.

For information on how to upload an intermediate certificate file, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see “Permissions” on page 47.

Syntax

```
config system certificate intermediate-certificate
  edit <int-certificate_name>
    set comment "<comment_str>"
  next
end
```

Variable	Description	Default
<int-certificate_name>	Type the name of an intermediate certificate file. The maximum length is 35 characters.	No default.
comment "<comment_str>"	Type a description or other comment. If the comment is more than one word or contains an apostrophe, surround the comment with double quotes ("). The maximum length is 127 characters.	No default.

Related topics

- [config system certificate intermediate-certificate-group](#)
- [config server-policy policy](#)

system certificate intermediate-certificate-group

Use this command to group intermediate CA certificates.

Intermediate CAs must belong to a group in order to be selected in a certificate verification rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system certificate intermediate-certificate-group
  edit <intermediate-ca-group_name>
    config members
      edit <intermediate-ca_index>
        set name <ca_name>
      next
    end
  next
end
```

Variable	Description	Default
<intermediate-ca-group_name>	Type the name of an intermediate certificate authority (CA) group. The maximum length is 35 characters.	No default.
<intermediate-ca_index>	Type the index number of an intermediate CA within its group. The valid range is from 1 to 9,999,999,999,999,999.	No default.
name <ca_name>	Type the name of a previously uploaded intermediate CA certificate. The maximum length is 35 characters.	No default.

Related topics

- [config system certificate intermediate-certificate](#)
- [config server-policy policy](#)

system certificate local

Use this command to edit the comment associated with a server certificate that is stored locally on the FortiWeb appliance.

FortiWeb appliances require these certificates to present when clients request secure connections, including when:

- administrators connect to the web UI (HTTPS connections only)
- web clients use SSL or TLS to connect to a virtual server, if you have enabled SSL off-loading in the policy (HTTPS connections and reverse proxy mode)
- web clients use SSL or TLS to connect to a physical server (HTTPS connections and true transparent mode)

FortiWeb appliances also require certificates in order to decrypt and scan HTTPS connections travelling through it if operating in offline protection or transparent inspection modes.

Which certificate will be used, and how, depends on the purpose.

- For connections to the web UI, the FortiWeb appliance presents its default certificate.



The FortiWeb appliance's default certificate does not appear in the list of local certificates. It is used only for connections to the web UI and cannot be removed.

- For SSL off-loading or SSL decryption, upload certificates that do **not** belong to the FortiWeb appliance, but instead belong to the protected hosts. Then, select which one the FortiWeb appliance will use when configuring the SSL option in a policy or server farm.

For information on how to upload a certificate file, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config system certificate local
  edit <certificate_name>
    set comment "<comment_str>"
    set status {na | ok | pending}
    set type {certificate | csr}
    set flag {0 | 1}
  next
end
```

Variable	Description	Default
<certificate_name>	Type the name of a certificate file. The maximum length is 35 characters.	No default.
comment "<comment_str>"	Type a description or other comment. If the comment contains more than one word or contains an apostrophe, surround the comment in double quotes ("). The maximum length is 127 characters.	No default.

Variable	Description	Default
status {na ok pending}	Indicates the status of an imported certificate: <ul style="list-style-type: none"> na indicates that the certificate was successfully imported, and is currently selected for use by the FortiWeb appliance. ok indicates that the certificate was successfully imported but is not selected as the certificate currently in use. To use the certificate, select it in a policy or server farm. pending indicates that the certificate request was generated, but must be downloaded, signed, and imported before it can be used as a local certificate. 	No default.
type {certificate csr}	Indicates whether the file is a certificate or a certificate signing request (CSR).	No default.
flag {0 1}	Indicates if a password was saved. This is used by FortiWeb for backwards compatibility.	No default.

Example

This example adds a comment to the certificate named `certificate1`.

```
config system certificate local
    edit certificate1
        set comment "This is a certificate for the host www.example.com."
    next
end
```

Related topics

- [config server-policy policy](#)
- [config server-policy pservers](#)

system certificate remote

Use this command to edit the comment and URL associated with the certificates of the online certificate status protocol (OCSP) or HTTP CRL servers of your certificate authority (CA).

OCSP enables you to revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL).

For information on how to upload a certificate file, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config system certificate remote
edit <ocsp_name>
    set comment "<comment_str>"
    set ocsp_url <url_str>
next
end
```

Variable	Description	Default
<ocsp_name>	Type the name of an OCSP certificate file. The maximum length is 35 characters.	No default.
comment "<comment_str>"	Type a description or other comment. If the comment is more than one word or contains an apostrophe, surround the comment with double quotes ("). The maximum length is 127 characters.	No default.
ocsp_url <url_str>	If you want to query for the server's certificate from its URL, enter the URL of the server. The maximum length is 127 characters.	No default.

Related topics

- [config system certificate local](#)
- [config system certificate verify](#)

system certificate verify

Use this command to configure how the FortiWeb appliance will verify certificates presented by HTTP clients.

To apply a certificate verification rule, select it in a policy. For details, see [“config server-policy policy” on page 140](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system certificate verify
  edit <certificate_verificator_name>
    set ca <ca-group_name>
    set crl <crl_name>
    set ocsp <remote_name>
  next
end
```

Variable	Description	Default
<certificate_verificator_name>	Type the name of a certificate verifier. The maximum length is 35 characters.	No default.
ca <ca-group_name>	Type the name of a CA group, if any, that you want to use to authenticate client certificates. The maximum length is 35 characters.	No default.
crl <crl_name>	Type the name of a certificate revocation list, if any, to use to verify the revocation status of client certificates. The maximum length is 35 characters.	No default.
ocsp <remote_name>	Type the name of an OCSP or HTTP (remote) server certificate, if any, that you want to use to verify the revocation status of client certificates. The maximum length is 35 characters.	No default.

Related topics

- [config system certificate ca-group](#)
- [config system certificate crl](#)
- [config system certificate remote](#)
- [config server-policy policy](#)
- [config server-policy pservers](#)

system conf-sync

Use this command to configure non-HA configuration synchronization settings.



This command configures, but does **not** execute, the synchronization. To do this, use the web UI.

This command works only when administrative domains (ADOMs) are disabled.

This type of synchronization is used between FortiWeb appliances that are not part of a native FortiWeb high availability (HA) pair, such as when you need to clone the configuration once, or when HA is provided by an external device.

To use this command, your administrator account’s access control profile must have either w or rw permission to the sysgrp area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system conf-sync
    set ip <remote-fortiweb_ipv4>
    set password <password_str>
    set sync-type {full-sync | partial-sync}
    set server-port <port_int>
end
```

Variable	Description	Default
ip <remote-fortiweb_ipv4>	Type the IP address of the remote FortiWeb appliance that you want to synchronize with the local FortiWeb appliance.	0.0.0.0
password <password_str>	Type the administrator password for the remote FortiWeb appliance. The maximum length is 63 characters.	No default.

Variable	Description	Default
sync-type {full-sync partial-sync}	<p>Select one of the synchronization types:</p> <ul style="list-style-type: none"> full-sync — Update the entire configuration of the peer FortiWeb appliance except its network interfaces and administration configuration. Note: This option has no effect if the FortiWeb appliance is operating in reverse proxy mode. See “config system settings” on page 230. partial-sync — Update the configuration of the peer FortiWeb appliance, with the exception of: <pre>config system ... config router ... config server-policy ... commands for health, dserver, pserver, pservers, vserver, service, and http-content- routing-policy config server-policy policy (completely replaces the peer's policy)</pre> 	partial -sync
server-port <port_int>	<p>Type the port number of the remote (peer) FortiWeb appliance that is used to connect to the local appliance for configuration synchronization. The valid range is from 1 to 65,535.</p> <p>Caution: The port number used with this command must be different than the port number used with config system global command or the submitting operation will fail.</p>	8333

Related topics

- [config system settings](#)
- [config system global](#)

system console

Use this command to configure the management console settings. Usually this is set during the early stages of installation and needs no adjustment.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system console
  set baudrate {9600 | 19200 | 38400 | 57600 | 115200}
  set mode {batch | line}
  set output {more | standard}
end
```

Variable	Description	Default
baudrate {9600 19200 38400 57600 115200}	Select the baud rate of the console connection. The rate should conform to the specifications of your specific FortiWeb appliance.	9600
mode {batch line}	Select the console input mode: either batch or line.	line
output {more standard}	Select either: <ul style="list-style-type: none"><code>more</code> — When displaying multiple pages' worth of output, pause after displaying each page's worth of text. When the display pauses, the last line displays <code>--More--</code>. You can then either:<ul style="list-style-type: none">Press the spacebar to display the next page.Type <code>Q</code> to truncate the output and return to the command prompt.<code>standard</code> — Do not pause between pages' worth of output, and do not offer to truncate output.	standard
shell [cli sh}	Select either: <ul style="list-style-type: none"><code>cli</code> — Command-line shell.<code>sh</code> — Busybox shell.	cli

Example

This example configures the local console connection to operate at 9,600 baud, and to show long output in a paged format.

```
config system console
  set baudrate 9600
  set output more
end
```

Related topics

- [config system admin](#)

system dns

Use this command to configure the FortiWeb appliance with its local domain name, and the IP addresses of the domain name system (DNS) servers that the FortiWeb appliance will query to resolve domain names such as `www.example.com` into IP addresses.

FortiWeb appliances require connectivity to DNS servers for DNS lookups. Use either the DNS servers supplied by your Internet service provider (ISP) or the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Local host and broadcast addresses will not be accepted.



For improved performance, use DNS servers on your local network.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system dns
    set primary <dns_ipv4>
    set secondary <dns_ipv4>
    set domain <local-domain_str>
end
```

Variable	Description	Default
primary <dns_ipv4>	Type the IP address of the primary DNS server.	8.8.8.8
secondary <dns_ipv4>	Type the IP address of the secondary DNS server.	0.0.0.0
domain <local-domain_str>	Type the name of the local domain to which the FortiWeb appliance belongs, if any. The maximum length is 127 characters. This field is optional. It will not appear in the <code>Host :</code> field of HTTP headers for client connections to protected web servers. Note: You can also configure the host name. For details, see “config system global” on page 206 .	No default.

Example

This example configures the FortiWeb appliance with the name of the local domain to which it belongs, `example.com`. It also configures its host name, `fortiweb`. Together, this configures the FortiWeb appliance with its own fully qualified domain name (FQDN), `fortiweb.example.com`.

```
config system global
    set hostname "fortiweb"
end
config system dns
    set domain example.com
end
```

Related topics

- [config log syslog-policy](#)
- [config router static](#)
- [config system interface](#)
- [config system global](#)
- [config server-policy policy](#)

system dos-prevention

Use this command to configure protection from TCP `SYN` flood-style denial of service (DoS) attacks. Once you configure DoS protection, the FortiWeb appliance automatically applies it to connections matching any server policy.



For true transparent mode, use the `syncookie` and `half-open-threshold` options of server policy instead. See [“server-policy policy” on page 140](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system dos-prevention
    set syncookie {enable | disable}
    set half-open-threshold <syn-rate_int>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
end
```

Variable	Description	Default
<code>syncookie {enable disable}</code>	Enable to detect TCP <code>SYN</code> flood attacks.	<code>disable</code>
<code>half-open-threshold <syn-rate_int></code>	Type the maximum number of TCP <code>SYN</code> packets, including retransmission, that may be sent per second to a destination address. If this threshold is exceeded, the FortiWeb appliance treats the traffic as a DoS attack and ignores additional traffic from that source address. The valid range is from 10 to 10,000 packets.	100
<code>severity {High Medium Low}</code>	Select the severity level to use in logs and reports generated when a violation of the policy occurs.	High
<code>trigger <trigger-policy_name></code>	Type the name of the trigger to apply when this policy is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: <code>set trigger ?</code>	No default.

Related topics

- [config waf application-layer-dos-prevention](#)
- [config log trigger-policy](#)

system fail-open

If your appliance's hardware model, network cabling, and configuration supports it, you can configure fail-to-wire/bypass behavior. This allows traffic to pass through unfiltered between 2 ports (a link pair) while the FortiWeb appliance is shut down, rebooting, or has unexpectedly lost power such as due to being accidentally unplugged or PSU failure.



Fail-open is supported **only**:

- in true transparent proxy mode or transparent inspection operation mode
- in standalone mode (**not** HA)
- for a bridge (V-zone) between ports wired to a CP7 processor or other hardware which provides support for fail-to-wire
 - FortiWeb 1000C: port3 + port4
 - FortiWeb 1000D: port3 + port4 and port5 + port6
 - FortiWeb 3000C/D: port5 + port6
 - FortiWeb 4000C/D: port5 + port6 and port7 + port8
 - FortiWeb 3000CFsx: port5 + port6 and port7 + port8
 - FortiWeb 3000DFsx: port5 + port6

FortiWeb 400B/400C, FortiWeb HA clusters, and ports not wired to a CP7/fail-open chip do **not** support fail-to-wire.



In the case of HA, don't use fail-open — instead, use a standby HA appliance to provide full fault tolerance.

Bypass results in degraded security while FortiWeb is shut down, and therefore HA is usually a better solution: it ensures that degraded security does not occur if one of the appliances is shut down. If it is possible that **both** of your HA FortiWeb appliance could simultaneously lose power, you can add an external bypass device such as [FortiBridge](#).

Fail-to-wire may be useful if you are required by contract to provide uninterrupted connectivity, or if you consider connectivity interruption to be a greater risk than being open to attack during the power interruption.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system fail-open
  set port3-port4 {poweroff-bypass | poweroff-cutoff}
end
```

Variable	Description	Default
port3-port4 {poweroff-bypass poweroff-cutoff}	Select either: <ul style="list-style-type: none">poweroff-bypass — Behave like a wire when powered off, allowing connections to pass directly through from one port to the other, bypassing policy and profile filtering.poweroff-keep — Interrupt connectivity when powered off. Note: The name of this setting varies by which ports are wired together for bypass in your specific hardware model.	poweroff-bypass

Related topics

- [config system ha](#)

system global

Use this command to configure the language, display refresh rate and listening ports of the web UI, the time zone and host name of the FortiWeb appliance, and NTP time synchronization.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system global
  set admin-port <port_int>
  set admin-sport <port_int>
  set admintimeout <minutes_int>
  set adom-admin {enable | disable}
  set auth-timeout <milliseconds_int>
  set cli-signature {enable | disable}
  set confsync-port <port_int>
  set dst {enable | disable}
  set hostname <host_name>
  set ie6workaround {enable | disable}
  set language {english | japanese | simch | trach}
  set no-ssl-renegotiation {enable | disable}
  set no-sslsv3 {enable | disable}
  set ntpserver {<ntp_fqdn> | <ntp_ipv4>}
  set ntpsync {enable | disable}
  set refresh <seconds_int>
  set single-admin-mode {enable | disable}
  set ssl-md5 {enable | disable}
  set strong-password {enable | disable}
  set syncinterval <minutes_int>
  set timezone <time-zone-code_str>
  set weak_enc {enable | disable}
end
```

Variable	Description	Default
admin-port <port_int>	Type the port number on which the FortiWeb appliance will listen for HTTP access to the web UI. The valid range is from 1 to 65,535.	80
admin-sport <port_int>	Type the port number on which the FortiWeb appliance will listen for HTTPS (SSL-secured) access to the web UI. The valid range is from 1 to 65,535.	443
admintimeout <minutes_int>	Type the amount of time in minutes after which an idle administrative session with the web UI or CLI will be automatically logged out. The valid range is from 1 to 480 minutes (8 hours). To improve security, do not increase the idle timeout.	5

Variable	Description	Default
<code>adom-admin</code> <code>{enable disable}</code>	<p>Enable to be able to restrict administrator accounts to specific administrative domains. See also domains <adom_name> in “config system admin” on page 170.</p> <p>Note: After you type <code>end</code>, if this setting is enabled, the CLI will terminate your session and restructure the configuration to use ADOMs. Global settings will remain in the global configuration scope, but objects that are configurable separately per ADOM such as services are moved to the <code>root</code> ADOM. To continue by configuring additional ADOMs, log in again, then go to “Defining ADOMs” on page 59.</p>	disable
<code>auth-timeout</code> <code><milliseconds_int></code>	<p>Type the number of milliseconds that FortiWeb will wait for the remote authentication server to respond to its query. The valid range is from 1 to 60,000 (60 seconds).</p> <p>If administrator logins often time out, and FortiWeb is configured to query an external RADIUS or LDAP server, increasing this value may help.</p> <p>This setting only affects remote authentication queries for administrator accounts. To configure the query connection timeout for end-user accounts, use <code>auth-timeout <timeout_int></code> in the HTTP authentication policy instead.</p>	2000
<code>cli-signature</code> <code>{enable disable}</code>	<p>Enable to be able to enter custom attack signatures via the CLI.</p> <p>Typically, attack signatures should be entered using the web UI, where you can verify syntax and test matching of your regular expression. If you are sure that your expression is correct, you can enable this option to enter your custom signature via the CLI.</p>	disable
<code>confsync-port</code> <code><port_int></code>	<p>Type the port number the local FortiWeb appliance uses to listen for a remote (peer) FortiWeb appliance when configured to synchronize its configuration. The valid range is from 1 to 65,535.</p> <p>Caution: The port number must be different than the port number set using <code>config system conf-sync</code>.</p>	8333
<code>dst {enable disable}</code>	<p>Enable to automatically adjust the FortiWeb appliance’s clock for daylight savings time (DST).</p>	disable

Variable	Description	Default
hostname <host_name>	<p>Type the host name of this FortiWeb appliance. Host names may include US-ASCII letters, numbers, hyphens, and underscores. The maximum length is 35 characters. Spaces and special characters are not allowed.</p> <p>The host name of the FortiWeb appliance is used in several places.</p> <ul style="list-style-type: none"> It appears in the <i>System Information</i> widget on the <i>Status</i> tab of the web UI, and in the get router all CLI command. It is used in the command prompt of the CLI. It is used as the SNMP system name. For information about SNMP, see “config system snmp sysinfo” on page 239. <p>The <i>System Information</i> widget and the get router all CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed.</p> <p>For example, if the host name is FortiWeb1234567890, the CLI prompt would be FortiWeb123456789~#.</p> <p>Note: You can also configure the local domain name. For details, see “config system dns” on page 201.</p>	FortiWeb
ie6workaround {enable disable}	<p>Enable to use the work around for a navigation bar freeze issue caused by using the web UI with Microsoft Internet Explorer 6.</p>	disable

Variable	Description	Default
language {english japanese simch trach}	<p>Select which language to use when displaying the web UI.</p> <p>The display's web pages will use UTF-8 encoding, regardless of which language you choose. UTF-8 supports multiple languages, and allows all of them to be displayed correctly, even when multiple languages are used on the same web page.</p> <p>For example, your organization could have web sites in both English and simplified Chinese. Your FortiWeb administrators prefer to work in the English version of the web UI. They could use the web UI in English while writing rules to match content in both English and simplified Chinese without changing this setting. Both the rules and the web UI will display correctly, as long as all rules were input using UTF-8.</p> <p>Usually, your text input method or your management computer's operating system should match the display, and also use UTF-8. If they do not, you may not be able to correctly display both your input and the web UI at the same time.</p> <p>For example, your web browser's or operating system's default encoding for simplified Chinese input may be GB2312. However, you usually should switch it to be UTF-8 when using the web UI, unless you are writing regular expressions that must match HTTP client's requests, and those requests use GB2312 encoding.</p> <p>For more information on language support in the web UI and CLI, see "Using the CLI Language support & regular expressions" on page 52.</p> <p>Note: This setting does not affect the display of the CLI.</p>	english
no-ssl- renegotiation {enable disable}	<p>Enable to prevent client-initiated SSL/TLS renegotiation.</p> <p>According to RFC 5246, either the client or the server can re-negotiate the connection in order to change cryptographic keys and other parameters. However, SSL/TLS renegotiation attacks exist to take advantage of the fact that the negotiation phase is more processing-intensive for the server than it is for the client. By repeatedly initiating renegotiations, clients can cause a DoS.</p>	
no-sslv3 {enable disable}	<p>Enable to disable support for SSL 3.0 connections to the web UI.</p> <p>Protects against a POODLE (Padding Oracle On Downgraded Legacy Encryption) attack.</p> <p>To disable access to back-end servers via SSL 3.0, use config system advanced.</p>	disable

Variable	Description	Default
ntpserver {<ntp_fqdn> <ntp_ipv4>}	Type the IP address or fully qualified domain name (FQDN) of a Network Time Protocol (NTP) server or pool, such as pool.ntp.org, to query in order to synchronize the FortiWeb appliance's clock. The maximum length is 63 characters. For more information about NTP and to find the IP address of an NTP server that you can use, see: http://www.ntp.org/	No default.
ntpsync {enable disable}	Enable to automatically update the system date and time by connecting to a NTP server. Also configure ntpserver {<ntp_fqdn> <ntp_ipv4>}, syncinterval <minutes_int> and timezone <time-zone-code_str>.	disable
refresh <seconds_int>	Type the automatic refresh interval, in seconds, for the web UI's <i>System Status Monitor</i> widget. The valid range is from 0 to 9,223,372,036,854,775,807 seconds. To disable automatic refreshes, type 0.	80
single-admin-mode {enable disable}	Enable to allow only one administrator account to be logged in at any given time. This option may be useful to prevent administrators from inadvertently overwriting each other's changes. When multiple administrators simultaneously modify the same part of the configuration, they each edit a copy of the current, saved state of the configuration item. As each administrator makes changes, FortiWeb does not update the other administrators' working copies. Each administrator may therefore make conflicting changes without being aware of the other. The FortiWeb appliance will only use whichever administrator's configuration is saved last. If only one administrator can be logged in at a time, this problem cannot occur. Disable to allow multiple administrators to be logged in. In this case, administrators should communicate with each other to avoid overwriting each other's changes.	disable
ssl-md5 {enable disable}	Enable if you need to support MD5 in HTTPS server policies. This option can be used to support older web browsers that require MD5 hashes and do not support SHA-1 or other hashes. See also weak_enc {enable disable}. Note: This option takes affect only if FortiWeb is operating in reverse proxy mode or true transparent proxy mode. Caution: Enabling this option weakens protection, and could make your servers susceptible to attacks involving MD5 in older versions of SSL. MD5 attacks are now trivial, and SHA-1 or stronger should be used if possible. If clients require SSL 2.0, which may use MD5, they are in violation of RFC 6176 . Enabling SSL 2.0 on the server is a violation of PCI DSS.	disable

Variable	Description	Default
<code>strong-password</code> {enable disable}	<p>Enable to enforce strong password rules for administrator accounts. If the password entered is not strong enough when a new administrator account is created, the FortiWeb appliance displays an error and prompts to enter a stronger password.</p> <p>Strong passwords have the following characteristics:</p> <ul style="list-style-type: none"> • are between 8 and 16 characters in length • contain at least one upper case and one lower case letter • contain at least one numeric • contain at least one non-alphanumeric character 	disable
<code>syncinterval</code> <minutes_int>	<p>Type how often, in minutes, the FortiWeb appliance should synchronize its time with the Network Time Protocol (NTP) server.</p> <p>The valid range is from 1 to 1440 minutes. To disable time synchronization, type 0.</p>	60
<code>timezone</code> <time-zone-code_str>	<p>Type the two-digit code for the time zone in which the FortiWeb appliance is located.</p> <p>The valid range is from 00 to 74. To display a list of time zone codes, their associated the GMT time zone offset, and contained major cities, type <code>set timezone ?</code>.</p>	00
<code>weak_enc</code> {enable disable}	<p>Enable if you need to support SSL 2.0 and 40- or 56-bit keys in HTTPS server policies. This option can be used to support older web browsers that do not support newer versions of SSL or TLS, and do not support greater key strengths. See also ssl-md5 {enable disable}.</p> <p>Note: This option takes affect only if FortiWeb is operating in reverse proxy mode or true transparent proxy mode.</p> <p>Caution: Enabling this option weakens encryption, and could make your servers susceptible to attacks on weak encryption. If clients require SSL 2.0, they are in violation of RFC 6176. Weak encryption is a violation of PCI DSS.</p>	disable

Example

This example configures time synchronization with a public NTP server pool. The FortiWeb appliance is located in the Pacific Time zone (code 04) and will synchronize its time with the NTP server pool every 60 minutes.

```
config system global
    set timezone 04
    set ntpsync enable
    set ntpserver pool.ntp.org
    set syncinterval 60
end
```

For an example that includes a host name, see [“config system dns”](#) on page 201.

Related topics

- [config system admin](#)
- [config system autoupdate schedule](#)
- [config system interface](#)
- [config system dns](#)
- [config system advanced](#)
- [config router static](#)
- [execute date](#)
- [execute time](#)
- [get system status](#)

system ha

Use this command to configure the FortiWeb appliance to act as a member of a high availability (HA) cluster in order to improve availability.

By default, FortiWeb appliances are each a single, standalone appliance. They operate independently.

If you have purchased more than one, however, you can configure the FortiWeb appliances to form an **active-passive** high availability (HA) FortiWeb cluster. This improves availability so that you can achieve your service level agreement (SLA) uptimes regardless of, for example, hardware failure or maintenance periods.



If you have multiple FortiWeb appliances but do **not** need failover, you can still synchronize the configuration. This can be useful for cloned network environments and externally load-balanced active-active HA. See [“config system conf-sync” on page 198](#).

HA requirements

- Two identical physical FortiWeb appliances (i.e., the same hardware model and firmware version (for example, both appliances could be a FortiWeb-3000C running FortiWeb))
- Redundant network topology: if the active appliance fails, physical network cabling and routes must redirect web traffic to the standby appliance
- At least one physical port on both HA appliances connected directly, via crossover cables, or through switches



FortiWeb-VM now supports HA. However, if you do not wish to use the native HA, you can use your hypervisor or VM environment manager to install your virtual appliances over a hardware cluster to improve availability. For example, VMware clusters can use vMotion or VMware HA.

The style of FortiWeb HA is **active-passive**: one appliance is elected to be the active appliance (also called the primary, main, or master), applying the policies for all connections. The other is a passive standby (also called the secondary, standby, or slave), which assumes the role of the active appliance and begins processing connections **only** if the active appliance fails.

For more information on HA, including troubleshooting, failover behavior, synchronized data, and network topology, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system ha
    set mode {active-passive | standalone}
    set group-id <group_int>
    [set group-name <pair-name_str>]
    set priority <level_int>
    set override {enable | disable}
    set hbdev <interface_name>
    [set hbdev-backup <interface_name>]
    set hb-interval <milliseconds_int>
    set hb-lost-threshold <seconds_int>
    set arps <arp_int>
    set arp-interval <seconds_int>
    [set monitor {<interface_name> ...}]
    set boot-time <limit_int>
end
```

Variable	Description	Default
mode {active-passive standalone}	<p>Select one of the following:</p> <ul style="list-style-type: none"> active-passive — Form an HA group with another FortiWeb appliance. The appliances operate together, with the standby assuming the role of the active appliance if it fails. standalone — Operate each appliance independently. 	standalone
group-id <group_int>	<p>Type a number that identifies the HA pair.</p> <p>Both members of the HA pair must have the same group ID. If you have more than one HA pair on the same network, each HA pair must have a different group ID.</p> <p>Changing the group ID changes the cluster's virtual MAC address. The valid range is 0 to 63.</p>	0
group-name <pair-name_str>	<p>Type a name to identify the HA pair if you have more than one. This setting is optional, and does not affect HA function. The maximum length is 35 characters.</p>	No default.
priority <level_int>	<p>Type the priority of the appliance when electing the primary appliance in the HA pair. (On standby devices, this setting can be reconfigured using the CLI command execute ha manage.)</p> <p>This setting is optional. The smaller the number, the higher the priority. The valid range is 0 to 9.</p> <p>Note: By default, unless you enable override {enable disable}, uptime is more important than this setting. For details, see the FortiWeb Administration Guide.</p>	5
override {enable disable}	<p>Enable to make priority <level_int> a more important factor than uptime when selecting the primary appliance.</p>	disable

Variable	Description	Default
hbdev <interface_name>	<p>Select which port on this appliance that the main and standby appliances will use to send heartbeat signals and synchronization data between each other (i.e. the HA heartbeat link). The maximum length is 15 characters.</p> <p>Connect this port to the same port number on the other member of the HA cluster. (e.g., If you select <code>port3</code> for the primary heartbeat link, connect <code>port3</code> on this appliance to <code>port3</code> on the other appliance.)</p> <p>At least one heartbeat interface must be selected on each appliance in the HA cluster. Ports that currently have an IP address assigned for other purposes (that is, virtual servers or bridges) cannot be re-used as a heartbeat link.</p> <p>At least one heartbeat interface must be selected on each appliance in the HA cluster. Ports that currently have an IP address assigned for other purposes (that is, virtual servers or bridges) cannot be re-used as a heartbeat link.</p> <p>Tip: If enough ports are available, you can select both a primary heartbeat interface and a secondary heartbeat interface (<code>hbdev-backup <interface_name></code>) on each appliance in the HA pair to provide heartbeat link redundancy. (You cannot use the same port as both the primary and secondary heartbeat interface on the same appliance, as this is incompatible with the purpose of link redundancy.)</p> <p>Note: If a switch is used to connect the heartbeat interfaces, the heartbeat interfaces must be reachable by Layer 2 multicast.</p>	No default.
hbdev-backup <interface_name>	<p>Select a secondary, standby port on this appliance that the main and standby appliances will use to send heartbeat signals and synchronization data between each other (i.e. the HA heartbeat link).</p> <p>It must not be the same network interface as <code>hbdev <interface_name></code>. The maximum length is 15 characters.</p> <p>Connect this port to the same port number on the other member of the HA cluster. (e.g., If you select <code>port4</code> for the secondary heartbeat link, connect <code>port4</code> on this appliance to <code>port4</code> on the other appliance.)</p> <p>Ports that currently have an IP address assigned for other purposes (that is, virtual servers or bridges) cannot be re-used as a heartbeat link.</p>	No default.

Variable	Description	Default
arps <arp_int>	<p>Type the number of times that the FortiWeb appliance will broadcast address resolution protocol (ARP) packets when it takes on the main role. (Even though a new NIC has not actually been connected to the network, FortiWeb does this to notify the network that a different physical port has become associated with the IP address and virtual MAC of the HA pair.) This is sometimes called “using gratuitous ARP packets to train the network,” and can occur when the main appliance is starting up, or during a failover. Also configure arp-interval <seconds_int>.</p> <p>Normally, you do not need to change this setting. Exceptions include:</p> <ul style="list-style-type: none"> • Increase the number of times the main appliance sends gratuitous ARP packets if your HA pair takes a long time to fail over or to train the network. Sending more gratuitous ARP packets may help the failover to happen faster. • Decrease the number of times the main appliance sends gratuitous ARP packets if your HA pair has a large number of VLAN interfaces and virtual domains. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair still fails over successfully, you could reduce the number of times gratuitous ARP packets are sent to reduce the amount of traffic produced by a failover. <p>The valid range is 1 to 16.</p>	3
arp-interval <seconds_int>	<p>Type the number of seconds to wait between each broadcast of ARP packets.</p> <p>Normally, you do not need to change this setting. Exceptions include:</p> <ul style="list-style-type: none"> • Decrease the interval if your HA pair takes a long time to fail over or to train the network. Sending ARP packets more frequently may help the failover to happen faster. • Increase the interval if your HA pair has a large number of VLAN interfaces and virtual domains. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair still fails over successfully, you could increase the interval between when gratuitous ARP packets are sent to reduce the rate of traffic produced by a failover. <p>The valid range is from 1 to 20.</p>	1

Variable	Description	Default
hb-interval <milliseconds_int>	<p>Type the number of 100-millisecond intervals to set the pause between each heartbeat packet that the one FortiWeb appliance sends to the other FortiWeb appliance in the HA pair. This is also the amount of time that a FortiWeb appliance waits before expecting to receive a heartbeat packet from the other appliance.</p> <p>This part of the configuration is synchronized between the active appliance and standby appliance.</p> <p>The valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds).</p> <p>Note: Although this setting is synchronized between the main and standby appliances, you should initially configure both appliances with the same <code>hb-interval <milliseconds_int></code> to prevent inadvertent failover from occurring before the initial synchronization.</p>	1
hb-lost-threshold <seconds_int>	<p>Type the number of times one of HA appliances retries the heartbeat and waits to receive HA heartbeat packets from the other HA appliance before assuming that the other appliance has failed.</p> <p>This part of the configuration is synchronized between the main appliance and standby appliance.</p> <p>Normally, you do not need to change this setting. Exceptions include:</p> <ul style="list-style-type: none"> • Increase the failure detection threshold if a failure is detected when none has actually occurred. For example, during peak traffic times, if the main appliance is very busy, it might not respond to heartbeat packets in time, and the standby appliance may assume that the main appliance has failed. • Reduce the failure detection threshold or detection interval if administrators and HTTP clients have to wait too long before being able to connect through the main appliance, resulting in noticeable down time. <p>The valid range is from 1 to 60.</p> <p>Note: Although this setting is synchronized between the main and standby appliances, you should initially configure both appliances with the same <code>hb-lost-threshold <seconds_int></code> to prevent inadvertent failover from occurring before the initial synchronization.</p> <p>Note: You can use SNMP traps to notify you when a failover is occurring. For details, see “config system snmp community” on page 234.</p>	3

Variable	Description	Default
monitor {<interface_name> ...}	<p>Type the name of one or more network interfaces that each directly correlate with a physical link. These ports will be monitored for link failure.</p> <p>Separate the name of each network interface with a space. To remove from or add to the list of monitored network interfaces, retype the entire list.</p> <p>Port monitoring (also called interface monitoring) monitors physical network ports to verify that they are functioning properly and linked to their networks. If the physical port fails or the cable becomes disconnected, a failover occurs. You can monitor physical interfaces,, but not VLAN subinterfaces or 4-port switches.</p> <p>Note: To prevent an unintentional failover, do not configure port monitoring until you configure HA on both appliances in the HA pair, and have plugged in the cables to link the physical network ports that will be monitored.</p>	No default.
boot-time <limit_int>	<p>Type the maximum number of seconds that a appliance will wait for a heartbeat or synchronization connection after the appliance returns online.</p> <p>If this limit is exceeded, the appliance will assume that the other unit is unresponsive, and assume the role of the main appliance.</p> <p>Due to the default heartbeat and synchronization intervals, as long as the HA pair are cabled directly together, the default value is usually sufficient. If the HA heartbeat link passes through other devices, such as routers and switches, however, a larger value may be needed. You may notice this especially when updating the firmware.</p> <p>The valid range is from 1 to 100 seconds.</p>	30

Example

This example configures a FortiWeb appliance as one appliance in an active-passive HA pair whose group ID is 1. The primary heartbeat occurs over port3, and the secondary heartbeat link is over port4. Priority is more important than uptime when electing the main appliance. The appliance will wait 30 seconds after boot time for a heartbeat or synchronization before

assuming that it should be that main appliance. Aside from the heartbeat link, failover can also be triggered by port monitoring of port1 and port2.

```
config system ha
    set mode active-passive
    set group-id 1
    set priority 6
    set override enable
    set hbdev port3
    set hbdev-backup port4
    set arps 3
    set arp-interval 2
    set hb-interval 1
    set hb-lost-threshold 3
    set monitor port1 port2
    set boot-time 30
end
```

Related topics

- [config system interface](#)
- [config system fail-open](#)
- [config system global](#)
- [diagnose debug application hasync](#)
- [diagnose debug application hataalk](#)
- [diagnose system ha status](#)
- [diagnose system ha mac](#)
- [execute ha disconnect](#)
- [execute ha manage](#)
- [execute ha synchronize](#)
- [get system status](#)

system interface

Use this command to configure:

- the network interfaces associated with the physical network ports of the FortiWeb appliance,
- VLAN subinterfaces or 802.3ad link aggregates associated with physical network interfaces

Both the network interfaces and VLAN subinterfaces can include administrative access.



You can restrict which IP addresses are permitted to log in as a FortiWeb administrator through the network interfaces and VLAN subinterfaces. For details, see [“config system admin” on page 170](#).



When the FortiWeb appliance is operating in either of the transparent modes, VLANs do not support Cisco discovery protocol (CDP).

You can use SNMP traps to notify you when a network interface’s configuration changes, or when a link is brought down or brought up. For details, see [“config system snmp community” on page 234](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system interface
edit <interface_name>
    set status {up | down}
    set type {aggregate | physical | vlan}
    set algorithm {layer2 | layer2_3 | layer3_4}
    set allowaccess {http https ping snmp ssh telnet}
    set ip6-allowaccess {http https ping snmp ssh telnet}
    set description "<comment_str>"
    set interface <interface_name>
    set intf {<port_name> ...}
    set ip <interface_ipv4mask>
    [set ip6 <interface_ipv6mask>]
    set mode static
    set vlanid <vlan-id_int>
```

```

        set lacp-speed {fast | slow}
    next
end

```

Variable	Description	Default
<interface_name>	Type the name of a network interface. The maximum length is 15 characters.	No default.
status {up down}	<p>Enable (select up) to bring up the network interface so that it is permitted to receive and/or transmit traffic.</p> <p>Note: This administrative status from this command is not the same as its detected physical link status.</p> <p>For example, even though you have used config system interface to configure port1 with set status up, if the cable is physically unplugged, diagnose hardware nic list port1 may indicate correctly that the link is down (Link detected: no).</p>	up
algorithm {layer2 layer2_3 layer3_4}	<p>Select the connectivity layers that will be considered when distributing frames among the aggregated physical ports.</p> <ul style="list-style-type: none"> • layer2 — Consider only the MAC address. This results in the most even distribution of frames, but may be disruptive to TCP if packets frequently arrive out of order. • layer2_3 — Consider both the MAC address and IP session. Queue frames involving the same session to the same port. This results in slightly less even distribution, and still does not guarantee perfectly ordered TCP sessions, but does result in less jitter within the session. • layer3_4 — Consider both the IP session and TCP connection. Queue frames involving the same session and connection to the same port. Distribution is not even, but this does prevent TCP retransmissions associated with link aggregation. 	layer2

Variable	Description	Default
allowaccess {http https ping snmp ssh telnet}	<p>Type the IPv4 protocols that will be permitted for administrative connections to the network interface or VLAN subinterface.</p> <p>Separate each protocol with a space. To remove from or add to the list of permitted administrative access protocols, retype the entire list.</p> <ul style="list-style-type: none"> • <code>ping</code> — Allow ICMP ping responses from this network interface. • <code>http</code> — Allow HTTP access to the web UI. Caution: HTTP connections are <i>not</i> secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail appliance, enable this option only on network interfaces connected directly to your management computer. • <code>https</code> — Allow secure HTTP (HTTPS) access to the web UI. • <code>snmp</code> — Allow SNMP access. For more information, see “config system snmp community” on page 234. Note: This setting only configures which network interface will <i>receive</i> SNMP queries. To configure which network interface will <i>send</i> traffic, see “config system snmp community” on page 234. • <code>ssh</code> — Allow SSH access to the CLI. • <code>telnet</code> — Allow Telnet access to the CLI. Caution: Telnet connections are <i>not</i> secure. <p>Caution: Enable administrative access only on network interfaces or VLAN subinterfaces that are connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiWeb appliance. Consider allowing ping only when troubleshooting.</p>	ping https ssh

Variable	Description	Default
ip6-allowaccess {http https ping snmp ssh telnet}	<p>Type the IPv6 protocols that will be permitted for administrative connections to the network interface or VLAN subinterface.</p> <p>Separate each protocol with a space. To remove from or add to the list of permitted administrative access protocols, retype the entire list.</p> <ul style="list-style-type: none"> ping — Allow ICMP ping responses from this network interface. http — Allow HTTP access to the web UI. Caution: HTTP connections are <i>not</i> secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail appliance, enable this option only on network interfaces connected directly to your management computer. https — Allow secure HTTP (HTTPS) access to the web UI. snmp — Allow SNMP access. For more information, see “config system snmp community” on page 234. Note: This setting only configures which network interface will <i>receive</i> SNMP queries. To configure which network interface will <i>send</i> traffic, see “config system snmp community” on page 234. ssh — Allow SSH access to the CLI. telnet — Allow Telnet access to the CLI. Caution: Telnet connections are <i>not</i> secure. <p>Caution: Enable administrative access only on network interfaces or VLAN subinterfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiWeb appliance. Consider allowing ping only when troubleshooting.</p>	ping
description "<comment_str>"	Type a description or other comment. If the comment is more than one word or contains an apostrophe, surround the comment with double quotes ("). The maximum length is 63 characters.	No default.
interface <interface_name>	<p>Type the name of the network interface with which the VLAN subinterface will be associated. The maximum length is 15 characters.</p> <p>This field is available only if type is vlan.</p>	No default.
intf {<port_name> ...}	<p>Type the names of 2 physical network interfaces or more that will be combined into the aggregate link. Only physical network interfaces may be aggregated. The maximum length is 15 characters each.</p> <p>This field is available only if type is vlan.</p>	No default.

Variable	Description	Default
ip <interface_ipv4mask>	Type the IPv4 address and netmask of the network interface, if any. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet. The default setting for port1 is 192.168.1.99 with a netmask of 255.255.255.0. Other ports have no default.	Varies by the interface.
ip6 <interface_ipv6mask>	Type the IPv6 address and netmask of the network interface, if any. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet.	::/0
lACP-speed {fast slow}	<p>Select the rate of transmission for the LACP frames (LACPUs) between FortiWeb and the peer device at the other end of the trunking cables, either:</p> <ul style="list-style-type: none"> • SLOW — Every 30 seconds. • FAST — Every 1 second. <p>Note: This must match the setting on the other device. If the rates do not match, FortiWeb or the other device could mistakenly believe that the other's ports have failed, effectively disabling ports in the trunk.</p>	slow

Variable	Description	Default
<code>type {aggregate physical vlan}</code>	<p>Indicates whether the interface is directly associated with a physical network port, or is instead a VLAN subinterface or link aggregate.</p> <p>The default varies by whether you are editing a network interface associated with a physical port (<code>physical</code>) or creating a new subinterface/aggregate (<code>vlan</code> or <code>aggregate</code>).</p>	Varies by the interface.
<code>vlanid <vlan-id_int></code>	<p>Type the VLAN ID of packets that belong to this VLAN subinterface.</p> <ul style="list-style-type: none"> If one physical network port (that is, a VLAN trunk) will handle multiple VLANs, create multiple VLAN subinterfaces on that port, one for each VLAN ID that will be received. If multiple different physical network ports will handle the same VLANs, on each of the ports, create VLAN subinterfaces that have the same VLAN IDs. <p>The VLAN ID is part of the tag that is inserted into each Ethernet frame in order to identify traffic for a specific VLAN. VLAN header addition is handled automatically, and does not require that you adjust the maximum transmission appliance (MTU). Depending on whether the device receiving a packet operates at Layer 2 or Layer 3 of the network, this tag may be added, removed or rewritten before forwarding to other nodes on the network.</p> <p>For example, a Layer 2 switch or FortiWeb appliance operating in either of the transparent modes would typically add or remove a tag when forwarding traffic among members of the VLAN, but would not route tagged traffic to a different VLAN ID. In contrast, a FortiWeb appliance operating in reverse proxy mode, inspecting the traffic to make routing decisions based upon higher-level layers/protocols, might route traffic between different VLAN IDs (also known as inter-VLAN routing) if indicated by its policy, such as if it has been configured to do WSDL-based routing.</p> <p>For the maximum number of interfaces, including VLAN subinterfaces, see the FortiWeb Administration Guide.</p> <p>This field is available only when <code>type</code> is <code>vlan</code>. The valid range is between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1q-compliant router or switch connected to the VLAN subinterface.</p> <p>Note: Inter-VLAN routing is not supported if the FortiWeb appliance is operating in either of the transparent modes. In that case, you must configure the same VLAN IDs on each physical network port.</p>	0

Example

This example configures the network interface named port1, associated with the first physical network port, with the IP address and subnet mask 10.0.0.1/24. It also enables ICMP ECHO (ping) and HTTPS administrative access to that network interface, and enables it.

```
config system interface
  edit "port1"
    set ip 10.0.0.1 255.255.255.0
    set allowaccess ping https
    set status up
  next
end
```

Example

This example configures the network subinterface named vlan_100, associated with the physical network interface port1, with the IP address and subnet mask 10.0.1.1/24. It does not allow administrative access.

```
config system interface
  edit "vlan_100"
    set type vlan
    set ip 10.0.1.1 255.255.255.0
    set status up
    set vlanid 100
    set interface port1
  next
end
```

Related topics

- [config system v-zone](#)
- [config router static](#)
- [config server-policy vserver](#)
- [config system snmp community](#)
- [config system admin](#)
- [config system ha](#)
- [config system network-option](#)
- [execute ping](#)
- [diagnose hardware nic](#)
- [diagnose network ip](#)
- [diagnose network sniffer](#)

system ip-detection

Use this command to configure how FortiWeb analyzes the identification (ID) field in IP packet headers in order to distinguish source IP addresses that are actually Internet connections shared by multiple clients, not single clients.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system ip-detection
    set share-ip-detection-level {low | medium | high}
end
```

Variable	Description	Default
share-ip-detection-level {low medium high}	Select how different packets' ID fields can be before FortiWeb will detect that the IP is shared by multiple clients.	low

Related topics

- [config system advanced](#)

system network-option

Use this command to configure system-wide TCP connection options.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system network-option
    set tcp-timestamp {enable | disable}
    set tcp-tw-recycle {enable | disable}
end
```

Variable	Description	Default
tcp-timestamp {enable disable}	<p>Enable to both:</p> <ul style="list-style-type: none">• verify whether clients' TCP timestamps are sequential• include TCP timestamps in packets from FortiWeb <p>Disabling this option can be useful when multiple clients are in front of a source NAT gateway such as a FortiGate. If it applies source NAT but forwards packets to FortiWeb without modifying the TCP timestamp, packets received from that source IP will appear to FortiWeb to have an unstable timestamp. FortiWeb will therefore drop out-of-sequence packets. Disabling therefore prevents packets dropped due to this cause, and can improve performance in that case.</p> <p>Caution: Disabling this option affects FortiWeb's dynamic calculation of TCP retransmission timeout (RTO) and therefore round trip time (RTT). If you disable the timestamp when it is not necessary, this can result in decreased application performance.</p>	enable
tcp-tw-recycle {enable disable}	<p>Enable to quickly recycle sockets that are ready to close (i.e. in the <code>TIME_WAIT</code> state per the TCP RFC).</p> <p>This option can be useful in networks with both sustained high load and bursts of new connection requests. If all sockets are busy, new connection requests may be refused. Enabling this option frees sockets more quickly.</p> <p>Caution: Enabling this option can cause issues with external load balancers and HA failover if they are not expecting the connection to close quickly. This can result in decreased application performance. Generally, it is safer to wait for sockets to safely close before they are reused.</p>	disable

Related topics

- [config system interface](#)
- [execute ping](#)
- [diagnose network ip](#)
- [diagnose network sniffer](#)

system raid

Use this command to configure the RAID level.

Currently, only RAID level 1 is supported, and only on the following models shipped with FortiWeb 4.0 MR1 or later:

- FortiWeb-1000B
- FortiWeb-1000C
- FortiWeb-1000D
- FortiWeb-3000C
- FortiWeb-3000D
- FortiWeb-4000C
- FortiWeb-4000D

On older appliances that have been upgraded to FortiWeb 4.0 MR1, RAID cannot be activated.



Back up the data regularly. RAID is not a substitute for regular backups. RAID 1 (mirroring) is designed to improve hardware fault tolerance, but cannot negate all risks.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system raid
    set level {raid1}
end
```

Variable	Description	Default
level {raid1}	Type the RAID level. Currently, only RAID level 1 is supported.	raid1

Example

This example sets RAID level 1.

```
config system raid
    set level raid1
end
```

Related topics

- [execute create-raid level](#)
- [execute create-raid rebuild](#)
- [diagnose hardware raid list](#)

system settings

Use this command to configure the operation mode and gateway of the FortiWeb appliance.

You will usually set the operation mode once, during installation. Exceptions include if you install the FortiWeb appliance in offline protection mode for evaluation purposes, before deciding to switch to another mode for more feature support in a permanent deployment.



Back up your configuration before changing the operation mode. Changing modes deletes any policies not applicable to the new mode, TCP SYN flood protection settings, all static routes, all V-zone (bridge) IPs, and all VLANs. You must re-cable your network topology to suit the operation mode, unless you are switching between the two transparent modes, which have similar network topology requirements.



The physical topology must match the operation mode. You may need to re-cable your deployment after changing this setting. For details, see the [FortiWeb Installation Guide](#).

There are four operation modes:

- **Reverse proxy** — Requests are destined for a virtual server's network interface and IP address on the FortiWeb appliance. The FortiWeb appliance applies the first applicable policy, then forwards permitted traffic to a real web server. The FortiWeb appliance logs, blocks, or modifies violations according to the matching policy and its protection profile.
Most features are supported.
- **Offline protection** — Requests are destined for a real web server instead of the FortiWeb appliance; traffic is duplicated to the FortiWeb through a span port. The FortiWeb appliance monitors traffic received on the virtual server's network interface (regardless of the IP address) and applies the first applicable policy. Because it is not inline with the destination, it does **not** forward permitted traffic. The FortiWeb appliance logs or blocks violations according to the matching policy and its protection profile. If FortiWeb detects a malicious request, it sends a TCP RST (reset) packet to the web server and client to attempt to terminate the connection. It does **not** otherwise modify traffic. (It cannot, for example, apply SSL, load-balance connections, or support user authentication.)



Unlike in reverse proxy mode or true transparent proxy mode, actions other than **Alert cannot** be guaranteed to be successful in offline protection mode. The FortiWeb appliance will attempt to block traffic that violates the policy by mimicking the client or server and requesting to reset the connection. However, the client or server may receive the reset request after it receives the other traffic due to possible differences in routing paths.



Most organizations do **not** permanently deploy their FortiWeb appliances in offline protection mode. Instead, they will use offline protection as a way to learn about their web servers' protection requirements and to form some of the appropriate configuration during a transition period, after which they will switch to one of the operation modes that places the appliance inline between all clients and all web servers.

Switching out of offline protection mode when you are done with transition can prevent bypass problems that can arise as a result of misconfigured routing. It also offers you the ability to offer some protection features that cannot be supported in a span port topology used with offline detection.

- **True transparent proxy** — Requests are destined for a real web server instead of the FortiWeb appliance. The FortiWeb appliance **transparently proxies** the traffic arriving on a

network port that belongs to a Layer 2 bridge, applies the first applicable policy, and lets permitted traffic pass through. The FortiWeb appliance logs, blocks, or modifies violations according to the matching policy and its protection profile. **No changes to the IP address scheme of the network are required.** This mode supports user authentication via HTTP but **not** HTTPS.

- **Transparent inspection** — Requests are destined for a real web server instead of the FortiWeb appliance. The FortiWeb appliance **asynchronously inspects** traffic arriving on a network port that belongs to a Layer 2 bridge, applies the first applicable policy, and lets permitted traffic pass through. The FortiWeb appliance logs or blocks traffic according to the matching policy and its protection profile, but does **not** otherwise modify it. (It cannot, for example, apply SSL, load-balance connections, or support user authentication.)



Unlike in reverse proxy mode or true transparent proxy mode, actions other than **Alert cannot** be guaranteed to be successful in transparent inspection mode. The FortiWeb appliance will attempt to block traffic that violates the policy. However, due to the nature of asynchronous inspection, the client or server may have already received the traffic that violated the policy.

The default operation mode is reverse proxy.

Feature support varies by operation mode. For details, see the [FortiWeb Administration Guide](#).

You can use SNMP traps to notify you if the operation mode changes. For details, see “[config system snmp community](#)” on page 234.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see “[Permissions](#)” on page 47.

Syntax

```
config system settings
    set opmode {offline-protection | reverse-proxy | transparent |
transparent-inspection}
    set stop-guimonitor {enable | disable}
    set stop-monitor {enable | disable}
    set gateway <router_ipv4>

end
```

Variable	Description	Default
opmode {offline-protection reverse-proxy transparent transparent-inspection}	<p>Select the operation mode of the FortiWeb appliance.</p> <p>If you have not yet adjusted the physical topology to suit the new operation mode, see the FortiWeb Administration Guide. You may also need to reconfigure IP addresses, VLANs, static routes, bridges, policies, TCP SYN flood prevention, and virtual servers, and on your web servers, enable or disable SSL.</p> <p>Note: If you select <code>offline-protection</code>, you can configure the port from which TCP RST (reset) commands are sent to block traffic that violates a policy. For details, see block-port <port_int>.</p>	reverse-proxy
gateway <router_ipv4>	<p>Type the IPv4 address of the default gateway.</p> <p>This setting is visible only if <code>opmode</code> is either <code>transparent</code> or <code>transparent-inspection</code>. FortiWeb will use the <code>gateway</code> setting to create a corresponding static route under config router static with the first available index number. Packets will egress through <code>port1</code>, the hard-coded management network interface for the transparent operation modes.</p>	none

Variable	Description	Default
stop-monitor {enable disable}	<p>Enable to stop the physical or domain server health check daemon (also called a “watchdog” daemon).</p> <p>The watchdog daemon monitors all the active policies by sending either HTTP or HTTPS requests to servers every 5 seconds. If the watchdog daemon fails to get successful response from the server for 3 consecutive times (a total of 15 seconds), it will restart the corresponding policy and create a debug log entry.</p> <p>Disable to resume the watchdog daemon.</p> <p>Tip: Enable this option if a server is experiencing extended downtime, or if its IP address or port number configuration is incorrect. The watchdog daemon will detect a traffic disruption and restart the policy if:</p> <ul style="list-style-type: none"> • a policy only forwards to one server (i.e., the policy uses either a single server, or a server farm that contains only one server), and • that server is unreachable <p>In the case of extended downtime, enabling this option can improve performance by disabling availability checks and policy restarts that would otherwise consume FortiWeb resources.</p> <p>Note: The watchdog daemon is available only in reverse proxy mode.</p> <p>Note: To create debug log entries, you must first enable debug logging. See “diagnose debug” on page 424.</p>	disable
stop-guimonitor {enable disable}	<p>Enable to configure FortiWeb to stop checking whether the process that generates the web UI (httpsd) is defunct (that is, a defunct or zombie process).</p> <p>In some cases, a process that has completed execution can still have an entry in the process table, which can create a resource leak.</p> <p>When this setting is disabled, FortiWeb checks the process and stops and reloads the web UI if it determines that the process is defunct.</p>	disable

Related topics

- [config server-policy policy](#)
- [config server-policy vserver](#)

system snmp community

Use this command to configure the FortiWeb appliance's SNMP agent to belong to an SNMP community, and to select which events will cause the FortiWeb appliance to generate SNMP traps.

The FortiWeb appliance's simple network management protocol (SNMP) agent allows queries for system information can send traps (alarms or event messages) to the computer that you designate as its SNMP manager. In this way you can use an SNMP manager to monitor the FortiWeb appliance. You can add the IP addresses of up to eight SNMP managers to each community, which designate the destination of traps and which IP addresses are permitted to query the FortiWeb appliance.

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiWeb appliance to belong to at least one SNMP community so that community's SNMP managers can query the FortiWeb appliance's system information and receive SNMP traps from the FortiWeb appliance.

You can add up to three SNMP communities. Each community can have a different configuration for queries and traps, and the set of events which trigger a trap. Use SNMP traps to notify the SNMP manager of a wide variety of types of events. Event types range from basic system events, such as high usage of resources, to when an attack type is detected or a specific rule is enforced by a policy.

Before you can use SNMP, you must activate the FortiWeb appliance's SNMP agent (see [“config system snmp sysinfo” on page 239](#)) and add it as a member of at least one community. You must also enable SNMP access on the network interface through which the SNMP manager will connect. (See [“config system interface” on page 220](#).)

On the SNMP manager, you must also verify that the SNMP manager is a member of the community to which the FortiWeb appliance belongs, and compile the necessary Fortinet proprietary management information blocks (MIBs) and Fortinet-supported standard MIBs. For information on MIBs, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system snmp community
edit <community_index>
    set status {enable | disable}
    set name <community_str>
    set events {cpu-high | intf-ip | log-full | mem-low | netlink-
down-status | netlink-up-status | policy-start | policy-stop |
pserver-failed | sys-ha-hbfail | sys-mode-change | waf-access-
attack | waf-amethod-attack | waf-blogin-attack | waf-hidden-
fields | waf-pvalid-attack | waf-signature-detection | waf-url-
access-attack | waf-spage-attack}
    set query-v1-port <port_int>
    set query-v1-status {enable | disable}
    set query-v2c-port <port_int>
    set query-v2c-status {enable | disable}
    set trap-v1-lport <port_int>
    set trap-v1-rport <port_int>
    set trap-v1-status {enable | disable}
```

```

set trap-v2c-lport <port_int>
set trap-v2c-rport <port_int>
set trap-v2c-status {enable | disable}
config hosts
    edit <snmp-manager_index>
        set interface <interface_name>
        set ip <manager_ipv4>
    next
end
next
end

```

Variable	Description	Default
<community_index>	Type the index number of a community to which the FortiWeb appliance belongs. The valid range is from 1 to 9,999,999,999,999,999.	No default.
status {enable disable}	Enable to activate the community. This setting takes effect only if the SNMP agent is enabled. For details, see “config system snmp sysinfo” on page 239 .	disable
name <community_str>	Type the name of the SNMP community to which the FortiWeb appliance and at least one SNMP manager belongs. The maximum length is 35 characters. The FortiWeb appliance will not respond to SNMP managers whose query packets do not contain a matching community name. Similarly, trap packets from the FortiWeb appliance will include community name, and an SNMP manager may not accept the trap if its community name does not match.	No default.

Variable	Description	Default
events {cpu-high intf-ip log-full mem-low netlink- down-status netlink-up-status policy-start policy-stop pserver-failed sys-ha-hbfail sys-mode-change waf-access-attack waf-amethod-attack waf-blogin- attack waf-hidden- fields waf-pvalid- attack waf- signature- detection waf-url- access-attack waf- spage-attack	<p>Type one or more of the following SNMP event names in order to cause the FortiWeb appliance to send traps when those events occur. Traps will be sent to the SNMP managers in this community. Also enable traps.</p> <ul style="list-style-type: none"> • <code>cpu-high</code> — CPU usage has exceeded 80%. • <code>intf-ip</code> — A network interface's IP address has changed. See “config system interface” on page 220. • <code>log-full</code> — Local log disk space usage has exceeded 80%. If the space is consumed and a new log message is triggered, the FortiWeb appliance will either drop it or overwrite the oldest log message, depending on your configuration. See “config log disk” on page 70. • <code>mem-low</code> — Memory (RAM) usage has exceeded 80%. • <code>netlink-down-status</code> — A network interface has been brought down (disabled). This could be due to either an administrator changing the network interface's settings, or due to HA executing a failover. • <code>netlink-up-status</code> — A network interface has been brought up (enabled). This could be due to either an administrator changing the network interface's settings, or due to HA executing a failover. • <code>policy-start</code> — A policy was enabled. See “config server-policy policy” on page 140. • <code>policy-stop</code> — A policy was disabled. See “config server-policy policy” on page 140. • <code>pserver-failed</code> — A server health check has determined that a physical server that is a member of a server farm is now unavailable. See “config server-policy policy” on page 140. • <code>sys-ha-hbfail</code> — An HA failover is occurring. See “config system ha” on page 213. • <code>sys-mode-change</code> — The operation mode was changed. See “config system settings” on page 230. • <code>waf-access-attack</code> — FortiWeb enforced a page access rule. See “config waf page-access-rule” on page 350. • <code>waf-amethod-attack</code> — FortiWeb enforced an allowed methods restriction. See “config waf web-protection-profile inline-protection” on page 390, “config waf web-protection-profile offline-protection” on page 406, and “config waf allow-method-exceptions” on page 260. • <code>waf-blogin-attack</code> — FortiWeb detected a brute force login attack. See “config waf brute-force-login” on page 269. • <code>waf-hidden-fields</code> — FortiWeb detected a hidden fields attack. • <code>waf-pvalid-attack</code> — FortiWeb enforced an input/parameter validation rule. See “config waf parameter-validation-rule” on page 353. 	No default.

Variable	Description	Default
	<ul style="list-style-type: none"> waf-signature-detection — FortiWeb enforced a signature rule. See “config waf signature” on page 355. new waf-url-access-attack — FortiWeb enforced a URL access rule. See “config waf url-access url-access-rule” on page 374. new waf-spape-attack — FortiWeb enforced a start page rule. See “config waf start-pages” on page 368. 	
query-v1-port <port_int>	Type the port number on which the FortiWeb appliance will listen for SNMP v1 queries from the SNMP managers of the community. The valid range is from 1 to 65,535.	161
query-v1-status {enable disable}	Enable to respond to queries using the SNMP v1 version of the SNMP protocol.	enable
query-v2c-port <port_int>	Type the port number on which the FortiWeb appliance will listen for SNMP v2c queries from the SNMP managers of the community. The valid range is from 1 to 65,535.	161
query-v2c-status {enable disable}	Enable to respond to queries using the SNMP v2c version of the SNMP protocol.	enable
trap-v1-lport <port_int>	Type the port number that will be the source (also called local) port number for SNMP v1 trap packets. The valid range is from 1 to 65,535.	162
trap-v1-rport <port_int>	Type the port number that will be the destination (also called remote) port number for SNMP v1 trap packets. The valid range is from 1 to 65,535.	162
trap-v1-status {enable disable}	Enable to send traps using the SNMP v1 version of the SNMP protocol.	enable
trap-v2c-lport <port_int>	Type the port number that will be the source (also called local) port number for SNMP v2c trap packets. The valid range is from 1 to 65,535.	162
trap-v2c-rport <port_int>	Type the port number that will be the destination (also called remote) port number for SNMP v2c trap packets. The valid range is from 1 to 65,535.	162
trap-v2c-status {enable disable}	Enable to send traps using the SNMP v2c version of the SNMP protocol.	enable
<snmp-manager_index>	Type the index number of an SNMP manager for the community. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
interface <interface_name>	<p>Type the name of the network interface from which the FortiWeb appliance will send traps and reply to queries. The maximum length is 35 characters.</p> <p>Note: You must select a specific network interface if the SNMP manager is not on the same subnet as the FortiWeb appliance. This can occur if the SNMP manager is on the Internet or behind a router.</p> <p>Note: This setting only applies to the interface sending SNMP traffic. To configure the receiving interface, see config system interface.</p>	No default.
ip <manager_ipv4>	<p>Type the IP address of the SNMP manager that, if traps and/or queries are enabled in this community:</p> <ul style="list-style-type: none"> • will receive traps from the FortiWeb appliance • will be permitted to query the FortiWeb appliance <p>SNMP managers have read-only access.</p> <p>To allow any IP address using this SNMP community name to query the FortiWeb appliance, enter 0.0.0.0.</p> <p>Note: Entering 0.0.0.0 effectively disables traps if there are no other host IP entries, because there is no specific destination for trap packets. If you do not want to disable traps, you must add at least one other entry that specifies the IP address of an SNMP manager.</p>	No default.

Example

For an example, see “[config system snmp sysinfo](#)” on page 239.

Related topics

- [config system snmp sysinfo](#)
- [config system interface](#)
- [config server-policy policy](#)

system snmp sysinfo

Use this command to enable and configure basic information for the FortiWeb appliance's SNMP agent.

Before you can use SNMP, you must activate the FortiWeb appliance's SNMP agent and add it as a member of at least one community (see [“config system snmp community” on page 234](#)). You must also enable SNMP access on the network interface through which the SNMP manager will connect. (See [“config system interface” on page 220](#).)

On the SNMP manager, you must also verify that the SNMP manager is a member of the community to which the FortiWeb appliance belongs, and compile the necessary Fortinet proprietary management information blocks (MIBs) and Fortinet-supported standard MIBs. For information on MIBs, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system snmp sysinfo
    [set contact-info <contact_str>]
    [set description <description_str>]
    [set location <location_str>]
    set status {enable | disable}
end
```

Variable	Description	Default
contact-info <contact_str>	Type the contact information for the administrator or other person responsible for this FortiWeb appliance, such as a phone number or name. The contact information can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_). The maximum length is 35 characters.	No default.
description <description_str>	Type a description of the FortiWeb appliance. The string can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_). The maximum length is 35 characters.	No default.
location <location_str>	Type the physical location of the FortiWeb appliance. The string can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_). The maximum length is 35 characters.	No default.
status {enable disable}	Enable to activate the SNMP agent, enabling the FortiWeb appliance to send traps and/or receive queries for the communities in which you have enabled queries and/or traps. This setting enables queries only if SNMP administrative access is enabled on one or more network interfaces. For details, see “config system interface” on page 220 .	disable

Example

This example enables the SNMP agent, configures it to belong to a community named public whose SNMP manager is 172.168.1.20. The SNMP manager is not directly attached, but can be reached through the network interface named port3.

This example also configures the SNMP agent to send traps using SNMP v2c for high CPU or memory usage, and when the primary appliance fails; it also enables responses to SNMP v2c queries through the network interface named port3 (along with the previously enabled administrative access protocols, ICMP ping, HTTPS, and SSH).

```
config system snmp sysinfo
    set contact-info 'admin_example_com'
    set description 'FortiWeb-1000B'
    set location 'Rack_2'
    set status enable
end
config system snmp community
    edit 1
        set status enable
        set name public
        set events {cpu-high mem-low sys-ha-hbfail}
        set query-v1-status disable
        set query-v2c-port 161
        set query-v2c-status enable
        set trap-v1-status disable
        set trap-v2c-lport 162
        set trap-v2c-rport 162
        set trap-v2c-status enable
        config hosts
            edit 1
                set interface port3
                set ip 172.168.1.20
            next
        end
    next
end
config system interface
    edit port3
        set allowaccess ping https ssh snmp
    next
end
```

Related topics

- [config system snmp community](#)
- [config system interface](#)
- [config router static](#)

system v-zone

Use this command to configure bridged network interfaces, also called v-zones.

Bridges allow network connections to travel through the FortiWeb appliance's physical network ports **without** explicitly connecting to one of its IP addresses.

Bridges on the FortiWeb appliance support [IEEE 802.1d](#) spanning tree protocol (STP) by forwarding bridge protocol data unit (BPDU) packets, but do **not** generate BPDU packets of their own. Therefore, in some cases, you might need to manually test the bridged network for Layer 2 loops. Also, you may prefer to manually design a tree that uses the minimum cost path to the root switch for design and performance reasons.

True bridges typically have no IP address of their own. They use only media access control (MAC) addresses to describe the location of physical ports within the scope of their network and do network switching at Layer 2 of the OSI model. However, if you require the ability to use an IP address to use ICMP `ECHO_REQUEST` (ping) to test connectivity with the physical ports comprising the bridge, you can assign an IP address to the bridge using `ip <interface_ipv4mask>` and thereby create a virtual network interface that will respond.



For FortiWeb-VM, you must create vSwitches **before** you can configure a bridge. See the [FortiWeb-VM Install Guide](#) for details.



If configuring VLANs for a FortiWeb operating in true transparent proxy mode, you must configure one V-zone for each VLAN.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config system v-zone
  edit <bridge_name>
    set interfaces {<interface_name> <interface_name> ...}
```

```

    set ip <interface_ipv4mask>
  next
end

```

Variable	Description	Default
<bridge_name>	Type the name of the bridge. The maximum length is 15 characters. To display the list of existing bridges, type: edit ?	No default.
interfaces {<interface_name> <interface_name> ...}	Type the names of two or more network interfaces that currently have no IP address of their own, nor are members of another bridge, and therefore could be members of this bridge. Separate each name with a space. The maximum length is 35 characters.	No default.
ip <interface_ipv4mask>	To create a virtual network interface that can respond to ICMP ECHO (ping) requests, enter an IP address/subnet mask for the virtual network interface.	No default.

Example

This example configures a true bridge between port3 and port4. The bridge has no virtual network interface, and so it cannot respond to pings.

```

config system v-zone
  edit bridge1
    set interfaces port3 port4
  next
end

```

Related topics

- [config system interface](#)
- [config system settings](#)

user admin-usergrp

Use this command to configure LDAP or RADIUS remote authentication groups that can be used when configuring a FortiWeb administrator account.

Before you can add a remote authentication group, you must first define at least one query for either LDAP or RADIUS accounts. See [“config user ldap-user” on page 245](#) or [“config user radius-user” on page 252](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config user admin-usergrp
  edit <group_name>
    config members
      edit <entry_index>
        set type {ldap | radius}
        set ldap-name <query_name>
        set radius-name <query_name>
      next
    end
  next
end
```

Variable	Description	Default
<group_name>	Type the name of the remote authentication group. The maximum length is 35 characters.	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
type {ldap radius}	Select the protocol used for the query, either LDAP or RADIUS.	ldap
ldap-name <query_name>	Type the name of an existing LDAP account query. The maximum length is 35 characters. To display the list of existing queries, type: edit ?	No default.
radius-name <query_name>	Type the name of an existing RADIUS account query. The maximum length is 35 characters. To display the list of existing queries, type: edit ?	No default.

Example

This example creates a remote authentication group using an existing LDAP user query named LDAP Users 1. Because remote authentication groups use LDAP queries by default, the LDAP query type is not explicitly configured.

```
config user admin-usergrp
  edit "Admin LDAP"
```

```
    config members
      edit 0
        set ldap-name "LDAP Users 1"
      next
    end
  next
end
```

Related topics

- [config system admin](#)
- [config user ldap-user](#)
- [config user radius-user](#)
- [get system logged-users](#)

user ldap-user

Use this command to configure queries that can be used for remote authentication of either FortiWeb administrators or end users via an LDAP server.

To apply LDAP queries to end users, select a query in a user group that is then selected within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile used for web protection. For details, see [“config user user-group” on page 254](#).

To apply LDAP queries to administrators, select a query in an admin group and reference that group in a system administrator configuration. For details, see [“user admin-usergrp” on page 243](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config user ldap-user
edit <ldap-query_name>
    set bind-type {anonymous | simple | regular}
    set common-name-id <cn-attribute_str>
    set distinguished-name <search-dn_str>
    set filter <query-filter_str>
    set group_authentication {enable | disable}
    set group_dn <group-dn_str>
    set group-type {edirectory | open-ldap | windows-ad}
    set password <bind-password_str>
    set port <port_int>
    set protocol {ldaps | starttls}
    set server <ldap_ipv4>
    set ssl-connection {enable | disable}
```

```

set username <bind-dn_str>
next
end

```

Variable	Description	Default
<ldap-query_name>	Type the name of the LDAP user query. The maximum length is 35 characters. To display the list of existing queries, type: edit ?	No default.
bind-type {anonymous simple regular}	Select one of the following LDAP query binding styles: <ul style="list-style-type: none"> simple — Bind using the client-supplied password and a bind DN assembled from the common-name-id <cn-attribute_str>, distinguished-name <search-dn_str>, and the client-supplied user name. regular — Bind using a bind DN and password that you configure in username <bind-dn_str> and password <bind-password_str>. anonymous — Do not provide a bind DN or password. Instead, perform the query without authenticating. Select this option only if the LDAP directory supports anonymous queries. 	simple
common-name-id <cn-attribute_str>	Type the identifier, often cn, for the common name (CN) attribute whose value is the user name. The maximum length is 63 characters. Identifiers may vary by your LDAP directory's schema.	No default.
distinguished-name <search-dn_str>	Type the distinguished name (DN) such as ou=People,dc=example,dc=com, that, when prefixed with the common name, forms the full path in the directory to user account objects. The maximum length is 255 characters.	No default.
filter <query-filter_str>	Type an LDAP query filter string, if any, that will be used to filter out results from the query's results based upon any attribute in the record set. The maximum length is 255 characters. This option is valid only when bind-type is regular.	No default.
group_authentication {enable disable}	Enable to only include users that are members of an LDAP group. Also configure group-type {edirectory open-ldap windows-ad} and group_dn <group-dn_str> . This option is valid only when bind-type is regular.	enable
group_dn <group-dn_str>	Type the distinguished name of the LDAP user group, such as ou=Groups,dc=example,dc=com. The maximum length is 255 characters. This option is valid only when group_authentication is enabled.	No default.
group-type {edirectory open-ldap windows-ad}	Select the schema that matches your server's LDAP directory. Group membership attributes may have different names depending on an LDAP directory schemas. The FortiWeb appliance will use the group membership attribute that matches your directory's schema when querying the group DN. This option is valid only when group_authentication is enabled.	open-ldap

Variable	Description	Default
password <bind-password_str>	Type the password of the username <bind-dn_str> . The maximum length is 63 characters. This field may be optional if your LDAP server does not require the FortiWeb appliance to authenticate when performing queries, and does not appear if bind-type is anonymous or simple.	No default.
port <port_int>	Type the port number where the LDAP server listens. The valid range is from 1 to 65,535. The default port number varies by your selection in <code>ssl-connection</code> : port 389 is typically used for non-secure connections or for STARTTLS-secured connections, and port 636 is typically used for SSL-secured (LDAPS) connections.	389
protocol {ldaps starttls}	Select whether to secure the LDAP query using LDAPS or STARTTLS. You may need to reconfigure port <port_int> to correspond to the change in protocol. This field is applicable only if <code>ssl-connection</code> is enable.	ldaps
server <ldap_ipv4>	Type the IP address of the LDAP server.	0.0.0.0
ssl-connection {enable disable}	Enable to connect to the LDAP servers using an encrypted connection, then select the style of the encryption in protocol.	enable
username <bind-dn_str>	Type the bind DN, such as <code>cn=FortiWebA,dc=example,dc=com</code> , of an LDAP user account with permissions to query the distinguished-name <search-dn_str> . The maximum length is 255 characters. This field may be optional if your LDAP server does not require the FortiWeb appliance to authenticate when performing queries, and does not appear if bind-type is anonymous or simple.	No default.

Example

This example configures an LDAP user query to the server at 172.16.1.100 on port 389. SSL and TLS are disabled. To bind the query, the FortiWeb appliance will use the bind DN `cn=Manager,dc=example,dc=com`, whose password is `mySecretPassword`. Once connected and bound, the query for search for user objects in `ou=People,dc=example,dc=com`, comparing the user name supplied by the HTTP client to the value of each object's `cn` attribute. Group authentication is disabled.

```
config user ldap-user
    edit "ldap-user1"
        set server "172.16.1.100"
        set ssl-connection disable
        set port 389
        set common-name-id "cn"
        set distinguished-name "ou=People,dc=example,dc=com"
        set bind-type regular
        set username "cn=Manager,dc=example,dc=com"
        set password "mySecretPassword"
        set group-authentication disable
    next
end
```

Related topics

- [config user user-group](#)
- [config system admin](#)
- [config user admin-usergrp](#)

user local-user

Use this command to configure locally defined user accounts.

Local user accounts are used by the HTTP authentication feature to authorize HTTP requests. For details, see the [FortiWeb Administration Guide](#).

To incorporate local user accounts, add them to a user group that is selected within an authentication rule, which is in turn selected within an authentication policy. For details, see [“config user user-group” on page 254](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config user local-user
  edit <local-user_name>
    set username <user_str>
    set password <password_str>
  next
end
```

Variable	Description	Default
<local-user_name>	Type a name that can be referenced in other parts of the configuration. To display the list of existing accounts, type: <code>edit ?</code> Do not use spaces or special characters. The maximum length is 35 characters. Note: This is <i>not</i> the user name that the person must provide when logging in to the CLI or web UI.	No default.
username <user_str>	Type the user name that the client must provide when logging in, such as <code>user1</code> or <code>user1@example.com</code> . The maximum length is 63 characters.	No default.
password <password_str>	Type the password for the local user account. The maximum length is 63 characters.	No default.

Example

This example configures a local user account that can be used for HTTP authentication.

```
config user local-user
  edit "local-user1"
    set username "user1"
    set password "myPassword"
  next
end
```

Related topics

- [config user user-group](#)

user ntlm-user

Use this command to configure user accounts that will authenticate with the FortiWeb appliance via an NT LAN Manager (NTLM) server.

NTLM queries can be made to a Microsoft Windows or Active Directory server that has been configured for NTLM authentication. Both NTLM v1 and NTLM v2 versions of the protocol are supported.

NTLM user queries are used by the HTTP authentication feature to authorize HTTP requests. For details, see the [FortiWeb Administration Guide](#).

To incorporate NTLM user account queries, add them to a user group that is selected within an authentication rule, which is in turn selected within an authentication policy. For details, see [“config user user-group” on page 254](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config user ntlm-user
  edit <ntlm-query_name>
    set port <port_int>
    set server <ntlm_ipv4>
  next
end
```

Variable	Description	Default
<ntlm-query_name>	Type the name of the NTLM user query. The maximum length is 35 characters. To display the list of existing queries, type: <code>edit ?</code>	No default.
port <port_int>	Type the port number where the NTLM server listens. The valid range is from 1 to 65,535.	445
server <ntlm_ipv4>	Type the IP address of the NTLM server.	No default.

Example

This example configures an NTLM query connection to a server at 172.16.1.101 on port 445.

```
config user ntlm-user
  edit "ntlm-user1"
    set server "172.16.1.101"
    set port 445
  next
end
```

Related topics

- [config user user-group](#)

user radius-user

Use this command to configure RADIUS queries used to authenticate end-users and/or administrators.



If you use a RADIUS query for administrators, separate it from the queries for regular users. **Do not combine administrator and user queries into a single entry.** Failure to separate queries will allow end-users to have administrative access the FortiWeb web UI and CLI.

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. The FortiWeb authentication feature uses RADIUS user queries to authenticate and authorize HTTP requests. (The HTTP protocol does not support active logouts, and can only passively log out users when their connection times out. Therefore FortiWeb does **not** fully support RADIUS accounting.) RADIUS authentication with realms (i.e. the person logs in with an account such as admin@example.com) are supported.

To authenticate a user, the FortiWeb appliance sends the user's credentials to RADIUS for authentication. If RADIUS authentication succeeds, the user is successfully authenticated with the FortiWeb appliance. If RADIUS authentication fails, the appliance refuses the connection. To override the default authentication scheme, select a specific authentication protocol or change the default RADIUS port.

To incorporate RADIUS users, they must be in a user group selected within an authentication rule, which is in turn selected within an authentication policy. For details, see [“config user radius-user” on page 252](#).



For access profiles, FortiWeb appliances support [RFC 2548](#) Microsoft Vendor-specific RADIUS Attributes. If you do not want to use them, you can configure them locally instead. See [“config system accprofile” on page 167](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config user radius-user
edit <radius-query_name>
    set secret <password_str>
    set server <radius_ipv4>
    set server-port <port_int>
    set auth-type {default | chap | ms_chap | ms_chap_v2 | pap}
    set nas-ip <nas_ipv4>
    set secondary-secret <password_str>
    set secondary-server <radius2_ipv4>
```

```

    set secondary-server-port <port_int>
next
end

```

Variable	Description	Default
<radius-query_name>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters. To display the list of existing queries, type: edit ? Note: This is the name of the query only, not the administrator or end-user's account name/login, which is defined by either <administrator_name> or username <user_str>.	No default.
secret <password_str>	Type the RADIUS server secret key for the primary RADIUS server. The primary server secret key should be a maximum of 16 characters in length, but is allowed to be up to 63 characters.	No default.
server <radius_ipv4>	Type the IP address of the RADIUS server to query for users.	0.0.0.0
server-port <port_int>	Type the port number where the RADIUS server listens. The valid range is from 1 to 65,535.	1812
auth-type {default chap ms_chap ms_chap_v2 pap}	Type the authentication method. The default option uses PAP, MS-CHAP-V2, and CHAP, in that order.	default
nas-ip <nas_ipv4>	Type the NAS IP address and called station ID (see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address of the network interface that the FortiWeb appliance uses to communicate with the RADIUS server is applied.	0.0.0.0
secondary-secret <password_str>	Type the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key should be a maximum of 16 characters in length, but is allowed to be up to 63 characters.	No default.
secondary-server <radius2_ipv4>	Type the IP address of the secondary RADIUS server.	No default.
secondary-server-port <port_int>	Type the port number where the secondary RADIUS server listens. The valid range is from 1 to 65,535.	1812

Related topics

- [config user admin-usergrp](#)
- [config user user-group](#)

user user-group

Use this command to configure user groups.

User groups are used by the HTTP authentication feature to authorize HTTP requests. A group can include a mixture of local user accounts, LDAP, RADIUS, and NTLM user queries.

Before you can configure a user group, you must first configure any local user accounts or user queries that you want to include. For details, see [“config user local-user” on page 249](#), [“config user ldap-user” on page 245](#), [“config user radius-user” on page 252](#), or [“config user ntlm-user” on page 251](#).

To apply user groups, select them in within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile used for web protection. For details, see [“config waf http-authen http-authen-rule” on page 310](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config user user-group
edit <user-group_name>
    set auth-type {basic | digest | NTLM}
    config members
        edit <entry_index>
            set type {ldap | local | ntlm | radius}
            set ldap-name <query_name>
            set local-name <query_name>
            set ntlm-name <query_name>
            set radius-name <query_name>
        next
    end
next
end
```

Variable	Description	Default
<user-group_name>	Type the name of the user group. The maximum length is 35 characters. To display the list of existing groups, type: edit ?	No default.
auth-type {basic digest NTLM}	Select one of the following authentication types: <ul style="list-style-type: none">• <code>basic</code> — This is the original and most compatible authentication scheme for HTTP. However, it is also the least secure as it sends the user name and password unencrypted to the server.• <code>digest</code> — Authentication encrypts the password and thus is more secure than the basic authentication.• <code>NTLM</code> — Authentication uses a proprietary protocol of Microsoft and is considered to be more secure than basic authentication.	basic

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
ldap-name <query_name>	Select the name of a LDAP user query. Available if the value of <code>type</code> is <code>ldap</code> . The maximum length is 35 characters.	No default.
local-name <query_name>	Select the name of a local user account. Available if the value of <code>type</code> is <code>local</code> . The maximum length is 35 characters.	No default.
ntlm-name <query_name>	Select the name of a NTLM user query. Available if the value of <code>type</code> is <code>ntlm</code> . The maximum length is 35 characters.	No default.
radius-name <query_name>	Select the name of a RADIUS user query. Available if the value of <code>type</code> is <code>radius</code> . The maximum length is 35 characters.	No default.
type {ldap local ntlm radius}	Select which type of user or user query that you want to add to the group. Note: You can mix all user types in the group. However, if the authentication rule's <code>authen-type</code> does not support a given user type, all user accounts of that type will be ignored, effectively disabling them.	local

Example

For an example, see [“config waf http-authen http-authen-policy”](#) on page 307.

Related topics

- [config user ldap-user](#)
- [config user local-user](#)
- [config user ntlm-user](#)
- [config waf http-authen http-authen-rule](#)

wad website

Use this command to enable and configure web site defacement attack detection and automatic repair.

The FortiWeb appliance monitors the web site's files for any changes and folder modifications at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb appliance will notify you, and can quickly react by automatically restoring the web site contents to the previous backup revision.

Web site files will be backed up automatically and a revision will be created on the FortiWeb appliance in the following cases:

- When the FortiWeb appliance initiates monitoring for the first time, the FortiWeb appliance will download a backup copy of the web site's files and store it as the first revision.
- If the FortiWeb appliance could not successfully connect during a monitor interval, it will create a new revision the next time it re-establishes the connection.



When you intentionally modify the web site, you must disable the `monitor` option; otherwise, the FortiWeb appliance sees your changes as a defacement attempt and undoes them.



Backup copies will omit files exceeding the file size limit and/or matching the file extensions that you have configured the FortiWeb appliance to omit. See [backup-max-fsize <limit_int>](#) and [backup-skip-ftype <extensions_str>](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wadgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config wad website
  edit <entry_index>
    set alert-email <email-policy_name>
    set auto-restore {enable | disable}
    set backup-max-fsize <limit_int>
    set backup-skip-ftype <extensions_str>
    set connect-type {ftp | smb | ssh}
    set description "<comment_str>"
    set hostname-ip {<host_ipv4> | <host_fqdn>}
    set interval-other <seconds_int>
    set interval-root <seconds_int>
    set monitor {enable | disable}
    set monitor-depth <folders_int>
    set name <name_str>
    set password <password_str>
    set port <port_int>
    set share-name <share_str>
    set user <user_str>
```



```

set web-folder <path_str>
next
end

```

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 16.	No default.
alert-email <email-policy_name>	Type the name of the email policy that specifies the email address that FortiWeb sends an email to when it detects that the web site changed. (See “ config log email-policy ” on page 72.)The maximum length is 35 characters.	No default.
auto-restore {enable disable}	<p>Enable to automatically restore the web site to the previous revision number when it detects that the web site changed.</p> <p>Disable to do nothing. In this case, you must manually restore the web site to a previous revision when the FortiWeb appliance detects that the web site has been changed.</p> <p>Note: When you intentionally modify the web site, you must turn off this option; otherwise, the FortiWeb appliance will detect your changes as a defacement attempt, and undo them.</p>	disable
backup-max-fsize <limit_int>	<p>Type a file size limit in kilobytes (KB) to indicate which files will be included in the web site backup. Files exceeding this size will not be backed up. The valid range is from 1 to 1,048,576 kilobytes.</p> <p>Note: Backing up large files can impact performance.</p>	10240
backup-skip-ftype <extensions_str>	<p>Type zero or more file extensions, such as <i>iso</i>, <i>avi</i>, to exclude from the web site backup. Separate each file extension with a comma. The maximum length is 512 characters.</p> <p>Note: Backing up large files, such as video and audio, can impact performance.</p>	No default.
connect-type {ftp smb ssh}	Select which protocol to use when connecting to the web site in order to monitor its contents and download web site backups. For Microsoft Windows-style shares, enter <i>smb</i> .	ftp
description "<comment_str>"	Type a description or other comment. If the comment is more than one word or contains special characters, surround the comment with double quotes ("). The maximum length is 255 characters.	No default.
hostname-ip {<host_ipv4> <host_fqdn>}	<p>Type the IP address or fully qualified domain name (FQDN) of the physical server on which the web site is hosted.</p> <p>This will be used when connecting by SSH or FTP to the web site to monitor its contents and download backup revisions, and therefore could be different from the real or virtual web host name that may appear in the <i>Host :</i> field of HTTP headers.</p>	No default.
interval-other <seconds_int>	<p>Type the number of seconds between each monitoring connection from the FortiWeb appliance to the web server. During this connection, the FortiWeb appliance examines the web site's subfolders to see if any files have been changed by comparing the files with the latest backup. The valid range is from 1 to 86,400 seconds.</p> <p>If any file change is detected, the FortiWeb appliance will download a new backup revision. If you have enabled auto-restore {enable disable}, the FortiWeb appliance will revert the files to their previous version.</p>	600

Variable	Description	Default
interval-root <seconds_int>	Type the number of seconds between each monitoring connection from the FortiWeb appliance to the web server. During this connection, the FortiWeb appliance examines web-folder <path_str> (but not its subfolders) to see if any files have been changed by comparing the files with the latest backup. The valid range is from 1 to 86,400 seconds. If any file change is detected, the FortiWeb appliance will download a new backup revision. If you have enabled auto-restore {enable disable} , the FortiWeb appliance will revert the files to their previous version.	60
monitor {enable disable}	Enable to monitor the web site's files for changes, and to download backup revisions that can be used to revert the web site to its previous revision if the FortiWeb appliance detects a change attempt.	enable
monitor-depth <folders_int>	Type how many folder levels deep to monitor for changes to the web site's files. Files in subfolders deeper than this level will not be backed up. The valid range is from 1 to 10 levels deep.	5
name <name_str>	Type a name for the web site. The maximum length is 63 characters. This name will not be used when monitoring the web site, nor will it be referenced in any other part of the configuration, and therefore can be any identifier that is useful to you. It does not need to be the web site's FQDN or virtual host name.	No default.
password <password_str>	Type the password for the user name you entered in user <user_str> . The maximum length is 63 characters.	No default.
port <port_int>	Type the port number on which the web site's physical server listens. The standard port number for FTP is 21; the standard port number for SSH is 22. This is applicable only if <code>connect-type</code> is <code>ftp</code> or <code>ssh</code> .	21
share-name <share_str>	Type the name of the shared folder on the web server. The maximum length is 63 characters. This variable appears only if <code>connect-type</code> is <code>smb</code> .	No default.
user <user_str>	Type the user name that the FortiWeb appliance will use to log in to the web site's physical server. The maximum length is 63 characters.	No default.
web-folder <path_str>	Type the path to the web site's folder, such as <code>public_html</code> , on the physical server. The path is relative to the initial location when logging in with the user name that you specify in user <user_str> . The maximum length is 1,023 characters. Available only if the value of <code>connect-type</code> is <code>ftp</code> or <code>ssh</code> .	No default.

Example

```
config wad website
edit 1
    set alert-email email_policy_1
    set connect-type ssh
    set hostname-ip "192.168.1.10"
    set monitor enable
    set name "www.example.com"
    set password P@ssword1
```

```
        set port 22
        set user "fortiweb"
        set web-folder "public_html"
    next
end
```

Related topics

- [config system interface](#)
- [config router static](#)

waf allow-method-exceptions

Use this command to configure the FortiWeb appliance with combinations of URLs and host names, which are exceptions to HTTP request methods that are generally allowed or denied according to the inline or offline protection profile.

While most URL and host name combinations controlled by a profile may require similar HTTP request methods, you may have some that require different methods. Instead of forming separate policies and profiles for those requests, you can configure allowed method exceptions. The exceptions define specific HTTP request methods that are allowed by specific URLs and hosts.

To apply allowed method exceptions, select them within an inline or offline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#) or [“config waf web-protection-profile offline-protection” on page 406](#).

Before you configure an allowed method exception, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see [“config server-policy allow-hosts” on page 105](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf allow-method-exceptions
  edit <method-exception_name>
    config allow-method-exception-list
      edit <entry_index>
        set allow-request {connect delete get head options others post
        put trace}
        set host <protected-hosts_name>
        set host-status {enable | disable}
        set request-file <url_str>
        set request-type {plain | regular}
      next
    end
  next
end
```

Variable	Description	Default
<method-exception_name>	Type the name of the allowed methods exception. The maximum length is 35 characters. To display a list of the existing exceptions, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.

Variable	Description	Default
allow-request {connect delete get head options others post put trace}	<p>Select one or more of the allowed HTTP request methods that are an exception for that combination of URL and host.</p> <p>Methods that you do not select will be denied.</p> <p>The <i>OTHERS</i> option includes methods not specifically named in the other options. It often may be required by WebDAV (RFC 2518) applications such as Microsoft Exchange Server 2003 and Subversion, which may require HTTP methods not commonly used by web browsers, such as PROPFIND and BCOPY.</p> <p>Note: If a <i>WAF Auto Learning Profile</i> will be selected in the policy with an offline protection profile that uses this allowed method exception, you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb appliance to learn about. If a method is disabled, the FortiWeb appliance will reset the connection, and therefore cannot learn about the session.</p>	No default.
host <protected-hosts_name>	<p>Type the name of a protected host that the Host : field of an HTTP request must be in order to match the exception. The maximum length is 255 characters.</p> <p>This setting is used only if host-status is enable.</p>	No default.
host-status {enable disable}	Enable to require that the Host : field of the HTTP request match a protected hosts entry in order to match the allowed method exception. Also configure host <protected-hosts_name> .	disable
request-file <url_str>	<p>Depending on your selection in request-type {plain regular}, either:</p> <ul style="list-style-type: none"> Type the literal URL, such as /index.php, that is an exception to the generally allowed HTTP request methods. The URL must begin with a slash (/). Type a regular expression, such as ^/* .php, matching all and only the URLs which are exceptions to the generally allowed HTTP request methods. The pattern is not required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. <p>For example, if multiple URLs on a host have identical HTTP request method requirements, you would type a regular expression matching all of and only those URLs.</p> <p>Do not include the name of the web host, such as www.example.com, which is configured separately in host <protected-hosts_name>. The maximum length is 255 characters.</p> <p>Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the FortiWeb Administration Guide.</p>	No default.
request-type {plain regular}	Indicate whether request-file <url_str> is a literal URL (plain) or a regular expression (regular).	plain

Example

This example adds an exception to the list of allowed methods (post) that can be used in HTTP requests. In addition to the allowed methods already specified in protection profiles that use this exception, web hosts included in the protected hosts group named example_com_hosts

(such as example.com, www.example.com, and 192.168.1.10) are allowed to receive POST requests to the Perl file that handles the guestbook.

```
config waf allow-method-exceptions
  edit "auto-learn-profile2"
    config allow-method-exception-list
      edit 1
        set allow-request post
        set host "example_com_hosts"
        set host-status enable
        set request-file "/perl/guesbook.pl"
        set request-type plain
      next
    end
  next
end
```

Related topics

- [config server-policy allow-hosts](#)
- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)

waf allow-method-policy

Use this command to allow only specific HTTP request methods.

To define specific exceptions to this policy, use [config waf allow-method-exceptions](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf allow-method-policy
  edit <allowed-methods_name>
    set allow-method {connect delete get head options others post put
    trace}
    set severity {High | Medium | Low}
    set triggered-action <trigger-policy_name>
    set [allow-method-exception <method-exception_name>]
  next
end
```

Variable	Description	Default
<allowed-methods_name>	Type the name of a new or existing allowed methods policy. This field cannot be modified if you are editing an existing allowed method exception. To modify the name, delete the entry, then recreate it using the new name. The maximum length is 35 characters. To display a list of the existing policies, type: edit ?	No default.
allow-method {connect delete get head options others post put trace}	Select one or more HTTP request methods that you want to allow for this specific policy. Methods that you do not select will be denied, unless specifically allowed for a host and/or URL in [allow-method-exception <method-exception_name>] . The <i>OTHERS</i> option includes methods not specifically named in the other options. It often may be required by WebDAV (RFC 2518) applications such as Microsoft Exchange Server 2003 and Subversion , which may require HTTP methods not commonly used by web browsers, such as PROPFIND and BCOPY. Note: If a <i>WAF Auto Learning Profile</i> is used in the server policy where the HTTP request method is applied (via the <i>Web Protection Profile</i>), you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb appliance to learn about. If a method is disabled, the FortiWeb appliance will reset the connection, and therefore cannot learn about the session.	No default.

Variable	Description	Default
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the policy occurs.	High
triggered-action <trigger-policy_name>	Type the name of the trigger policy you want FortiWeb to apply when a violation of the HTTP request method policy occurs. Trigger policies determine who will be notified by email when the policy violation occurs, and whether the log message associated with the violation are recorded. The maximum length is 35 characters. To display a list of the existing policies, type: set triggered-action ?	No default.
[allow-method-exception <method-exception_name>]	Type the name of an existing HTTP request method exception, if any, to apply to it. The maximum length is 35 characters. To display a list of the existing policy, type: set allow-method-exception ?	No default.

Example

This example allows the HTTP GET and POST methods and rejects others, except according to the exceptions defined in MethodExceptions1.

```
config waf allow-method-policy
  edit "allowpolicy1"
    set allow-method get post
    set triggered-action "TriggerActionPolicy1"
    set allow-method-exception "MethodExceptions1"
  next
end
```

Related topics

- [config waf allow-method-exceptions](#)

waf application-layer-dos-prevention

Use this command to create an HTTP-layer DoS protection policy. Once you create the policy, reference it in an inline protection profile that is used by a server policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config waf application-layer-dos-prevention
edit <app-dos-policy_name>
    set enable-http-session-based-prevention {enable | disable}
    set http-connection-flood-check-rule <rule_name>
    set http-request-flood-prevention-rule <rule_name>
    set enable-layer4-dos-prevention {enable | disable}
    set layer4-access-limit-rule <rule_name>
    set layer4-connection-flood-check-rule <rule_name>
next
end
```

Variable	Description	Default
<app-dos-policy_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
enable-http-session-based-prevention {enable disable}	Enable to use DoS protection based on session cookies. Also configure http-connection-flood-check-rule <rule_name> and http-request-flood-prevention-rule <rule_name> .	disable
http-connection-flood-check-rule <rule_name>	Type the name of an existing rule that sets the maximum number of HTTP requests per second to a specific URL. The maximum length is 35 characters. To display a list of the existing rules, type: <code>set http-connection-flood-check-rule ?</code> This setting applies only if <code>enable-http-session-based-prevention</code> is enabled.	No default.
http-request-flood-prevention-rule <rule_name>	Type the name of an existing rule that limits TCP connections from the same client. The maximum length is 35 characters. To display a list of the existing rules, type: <code>set http-request-flood-prevention-rule ?</code> This setting applies only if <code>enable-http-session-based-prevention</code> is enabled.	No default.

Variable	Description	Default
enable-layer4-dos-prevention {enable disable}	Enable to use D oS protection that is not based on session cookies. Also configure layer4-access-limit-rule <rule_name> and layer4-connection-flood-check-rule <rule_name> .	disable
layer4-access-limit-rule <rule_name>	Type the name of a rule that limits the number of HTTP requests per second from any source IP address. The maximum length is 35 characters. To display a list of the existing rules, type: set layer4-access-limit-rule ? This setting applies only if enable-layer4-dos-prevention is enabled.	No default.
layer4-connection-flood-check-rule <rule_name>	Type the name of an existing rule that limits the number of TCP connections from the same source IP address. The maximum length is 35 characters. To display a list of the existing rules, type: set layer4-connection-flood-check-rule ? This setting applies only if enable-layer4-dos-prevention is enabled.	No default.

Example

This example shows the settings for a DoS protection policy that protects a web portal using existing DoS prevention rules.

```
config waf application-layer-dos-prevention
  edit "Web Portal DoS Policy"
    set enable-http-session-based-prevention enable
    set http-connection-flood-check-rule "Web Portal TCP Connect Limit"
    set http-request-flood-prevention-rule "Web Portal HTTP Request Limit"
    set enable-layer4-dos-prevention enable
    set layer4-access-limit-rule "Web Portal HTTP Request Limit"
    set layer4-connection-flood-check-rule "Web Portal Network Connect Limit"
  next
end
```

Related topics

- [config waf http-connection-flood-check-rule](#)
- [config waf http-request-flood-prevention-rule](#)
- [config waf layer4-access-limit-rule](#)
- [config waf layer4-connection-flood-check-rule](#)
- [config system dos-prevention](#)
- [config system advanced](#)
- [config system global](#)

waf base-signature-disable

Use this command to disable individual or whole categories of data leak and attack signatures in every signature group that currently exists.

For example, if you disable a certain signature ID with this command, the signature ID in every signature group you have defined will be disabled.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf base-signature-disable
  edit <signature-ID_name>
  next
end
```

Variable	Description	Default
<signature-ID_name>	Type the name of an individual signature or signature category ID. The maximum length is 35 characters. For example, to disable the first cross-site scripting attack signature everywhere it is currently selected, you would type: <code>edit 010000001</code>	No default.

Example

This example globally disables the XSS signature whose ID is 010000001.

```
config waf base-signature-disable
  edit "010000001"
  next
end
```

Related topics

- [config waf signature](#)

waf brute-force-login

Use this command to configure brute force login attack sensors.

Brute force attacks attempt to penetrate systems by the sheer number of clients, attempts, or computational power, rather than by intelligent insight. For example, in brute force attacks on authentication, multiple web clients may rapidly try one user name and password combination after another in an attempt to eventually guess a correct login and gain access to the system. In this way, behavior differs from web crawlers, which typically do not focus on a single URL.

Brute force login attack sensors track the rate at which each source IP address makes requests for specific URLs. If the source IP address exceeds the threshold, the FortiWeb appliance penalizes the source IP address by blocking additional requests for the time period that you indicate in the sensor.

To apply a brute force login attack sensor, select it within an inline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#).

You can use SNMP traps to notify you when a brute force login attack is detected. For details, see [“config system snmp community” on page 234](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf brute-force-login
  edit <brute-force-login_name>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    config login-page-list
      edit <entry_index>
        set access-limit-standalone-ip <rate_int>
        set access-limit-share-ip <rate_int>
        set block-period <seconds_int>
        set host <allowed-hosts_name>
        set host-status {enable | disable}
        set request-file <url_str>
      next
    end
  next
end
```

Variable	Description	Default
<brute-force-login_name>	Type the name of a new or existing brute force login attack sensor. The maximum length is 35 characters. To display a list of the existing sensor, type: edit ?	No default.
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	High

Variable	Description	Default
trigger <trigger-policy_name>	Type the name of the trigger to apply when this policy is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
access-limit-standalone-ip <rate_int>	Type the rate threshold for source IP addresses that are single clients. Request rates exceeding the threshold will cause the FortiWeb appliance to block additional requests for the length of the time in block-period <seconds_int> . The valid range is from 0 to 9,999,999,999,999,999. To disable the rate limit, type 0.	1
access-limit-share-ip <rate_int>	Type the rate threshold for source IP addresses that are shared by multiple clients behind a network address translation (NAT) device such as a firewall or router. Request rates exceeding the threshold will cause the FortiWeb appliance to block additional requests for the length of the time in the block-period <seconds_int> . The valid range is from 0 to 9,999,999,999,999,999. To disable the rate limit, type 0. Note: Blocking a shared source IP address could block innocent clients that share the same source IP address with an offending client. In addition, the rate is a total rate for all clients that use the same source IP address. For these reasons, you should usually enter a greater value for this field than for access-limit-share-ip <rate_int> .	1
block-period <seconds_int>	Type the length of time for which the FortiWeb appliance will block additional requests after a source IP address exceeds a rate threshold. The block period is shared by all clients whose traffic originates from the source IP address. The valid range is from 1 to 10,000 seconds.	1
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
host <allowed-hosts_name>	Type the name of a protected host that the Host : field of an HTTP request must be in order to match the sensor. The maximum length is 255 characters. This setting is applied only if host-status is enable.	No default.
host-status {enable disable}	Enable to require that the Host : field of the HTTP request match a protected hosts entry in order to be included in the brute force login attack sensor's rate calculations. Also configure host <allowed-hosts_name> .	disable
ip-port-enable {enable disable}	Enable to apply the limit of login attempts specified by access-limit-standalone-ip or access-limit-share-ip per TCP/IP session. When the value is disable, the limit is applied per source IP. Tip: If you need to cover both possibilities, create two members.	disable
request-file <url_str>	Type the literal URL, such as /login.php, that the HTTP request must match to be included in the brute force login attack sensor's rate calculations. The URL must begin with a slash (/). Do not include the name of the web host, such as www.example.com, which is configured separately in host <allowed-hosts_name> . The maximum length is 255 characters.	No default.

Example

This example limits IP addresses of individual HTTP clients to 3 requests per second, and NAT IP addresses to 20 requests per second, when they request the file login.php on the host www.example.com on TCP port 8080.

```
config waf brute-force-login
  edit "brute_force_attack_sensor"
    set access-limit-share-ip 20
    set access-limit-standalone-ip 3
    set block-period 120
    config login-page-list
      edit 1
        set host "www.example.com:8080"
        set host-status enable
        set request-file "/login.php"
      next
    end
  next
end
```

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config system snmp community](#)
- [config waf application-layer-dos-prevention](#)
- [config log trigger-policy](#)

waf custom-access policy

Use this command to configure custom access policies.

Custom access policies group custom access rules.

To apply a custom access policy, select it within an inline protection profile or offline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#) or [“config waf web-protection-profile offline-protection” on page 406](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf custom-access policy
  edit <custom-policy_name>
    config rule
      edit <entry_index>
        set rule-name "<custom-rule_name>"
      next
    end
  next
end
```

Variable	Description	Default
<custom-policy_name>	Type the name of a new or existing custom policy. The maximum length is 35 characters. To display a list of the existing policies, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,223,372,036,854,775,807.	No default.
rule-name "<custom-rule_name>"	Type the name of the existing custom access rule to add to the policy. The maximum length is 35 characters.	No default.

Example

For an example, see [“config waf custom-access rule” on page 273](#).

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config waf custom-access rule](#)

waf custom-access rule

Use this command to configure custom access rules.

What if you want to allow a web crawler, but only if it is not too demanding, and comes from a source IP that is known to be legitimate for that crawler? What if you want to allow only a client that is a senior manager's IP, and only if it hasn't been infected by malware whose access rate is contributing to a DoS?

Advanced access control rules provide a degree of flexibility for these types of complex conditions. You can combine any or all of these criteria:

- source IP
- rate limit
- HTTP header such as `X-Real-IP`:
- URL line in the HTTP header

In the rule, add all criteria that you require allowed traffic to match.

Before you can apply a custom access rule, you must first group it with any others that you want to apply in a custom access policy. For details, see [“config waf custom-access policy” on page 272](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf custom-access rule
edit <custom-access_name>
    set action {alert | alert_deny | block-period}
    set block-period <seconds_int>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    config access-limit-filter
        edit <entry_index>
            set access-rate-limit <rate_int>
        end
    end
    config http-header-filter
        edit <entry_index>
            set header-name-type {custom | predefined}
            set predefined-header {host | connection | authorization | x-
pad | cookie | referer | user-agent | X-Forwarded-For |
Accept}
            set pre-header-type {plain | regular}
            set pre-header-rev-match {enable | disable}
            set custom-header-name <key_str>
            set cus-header-type {plain | regular}
            set cus-header-rev-match {enable | disable}
            set header-value <value_str>
        end
    end
end
```

```

config source-ip-filter
    edit <entry_index>
        set source-ip {address_ipv4 | address_ipv6}
    end
config url-filter
    edit <entry_index>
        set request-file <url_str>
        set reverse-match {no | yes}
    end
config http-transaction
    edit <entry_index>
        set http-transation-timeout <timeout_int>
    end
config response-code
    edit <entry_index>
        set response-code-min <response-code_int>
        set response-code-max <response-code_int>
    end
config packet-interval
    edit <entry_index>
        set packet-interval-timeout <timeout_int>
    end
config signature-class
    edit {0100000000 | 0200000000 | 0300000000 | 0400000000 |
        0500000000 | 0600000000 | 0900000000}
        set status {enable | disable}
config occurrence
    edit <entry_index>
        set occurrence-num <occurrence_int>
        set within <within_int>
        set traced-by {Source-IP | User}

```

```

end
next
end

```

Variable	Description	Default
<custom-access_name>	Type the name of a new or existing custom access rule. The maximum length is 35 characters. To display a list of the existing rule, type: edit ?	No default.
action {alert alert_deny block-period}	Select the specific action to be taken when the request matches the this signature. <ul style="list-style-type: none"> alert — Accept the request and generate an alert email and/or log message. Note: If type is data-leakage, does not cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) alert_deny — Block the request (or reset the connection) and generate an alert email and/or log message. This option is applicable only if type is signature-creation. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or error-msg <message_str> in “server-policy policy” on page 140. block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. 	alert
block-period <seconds_int>	Type the length of time for which the FortiWeb appliance will block additional requests after a source IP address violates this rule. The block period is shared by all clients whose traffic originates from the source IP address. The valid range is from 1 to 3,600 seconds.	60
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
trigger <trigger-policy_name>	Type the name of the trigger to apply when this policy is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
access-rate-limit <rate_int>	Type the rate threshold for source IP addresses. The valid range is from 0 to 9,999,999,999,999,999,999. To disable the rate limit, type 0. Note: Blocking a shared source IP address could block innocent clients that share the same source IP address with an offending client.	1

Variable	Description	Default
header-name-type {custom predefined}	<p>Select whether to define the HTTP header filter by selecting a predefined HTTP header name, or by typing the name of a custom HTTP header. Also configure header-value <value_str> and, depending on which you indicate in this option, either:</p> <ul style="list-style-type: none"> predefined-header {host connection authorization x-pad cookie referer user-agent X-Forwarded-For Accept} , pre-header-type {plain regular} , and pre-header-rev-match {enable disable} custom-header-name <key_str>, cus-header-type {plain regular}, and cus-header-rev-match {enable disable} 	predefined
predefined-header {host connection authorization x-pad cookie referer user-agent X-Forwarded-For Accept}	<p>Select the name (key) of the HTTP header such as <code>Accept</code> : that must be present in order for the request to be allowed.</p> <p>This field appears only if <code>header-name-type</code> is <code>predefined</code>.</p>	host
pre-header-type {plain regular}	<p>Indicate whether header-value <value_str> is a literal header value (<code>plain</code>) or a regular expression that indicates multiple possible valid header values (<code>regular</code>).</p>	plain
pre-header-rev-match {enable disable}	<p>Indicate how to use predefined-header {host connection authorization x-pad cookie referer user-agent X-Forwarded-For Accept} and header-value <value_str> when determining whether or not this condition has been met.</p> <ul style="list-style-type: none"> <code>no</code> — If the regular expression does match the request object, the condition is met. <code>yes</code> — If the regular expression does not match the request object, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (<code>!</code>). <p>If all conditions are met, the FortiWeb appliance will allow access.</p>	disable
custom-header-name <key_str>	<p>Type the name (key) without the trailing colon (<code>:</code>), such as <code>X-Real-IP</code>, of the HTTP header that must be present in order for the request to be allowed.</p> <p>This field appears only if <code>header-name-type</code> is <code>custom</code>.</p>	No default.
cus-header-type {plain regular}	<p>Indicate whether header-value <value_str> is a literal header value (<code>plain</code>) or a regular expression that indicates multiple possible valid header values (<code>regular</code>).</p>	plain
cus-header-rev-match {enable disable}	<p>Indicate how to use custom-header-name <key_str> and header-value <value_str> when determining whether or not this condition has been met.</p> <ul style="list-style-type: none"> <code>no</code> — If the regular expression does match the request object, the condition is met. <code>yes</code> — If the regular expression does not match the request object, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (<code>!</code>). <p>If all conditions are met, the FortiWeb appliance will allow access.</p>	disable

Variable	Description	Default
header-value <value_str>	<p>Depending on your selection in pre-header-type {plain regular}, either:</p> <ul style="list-style-type: none"> Type the literal header value, such as 172.0.2.80, your specified HTTP header must contain in order to match the filter. Value matching is case sensitive. (If you require a filter based upon more than one HTTP header, create multiple entries in the set, one for each HTTP header.). Type a regular expression, such as 172\.\0\.\2\.*, matching all and only the header values which accepted HTTP header values must match. <p>Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the FortiWeb Administration Guide.</p> <p>Tip: To prevent accidental matches, specify as much of the header's value as possible. Do not use an ambiguous substring.</p> <p>For example, entering the value 192.168.1.1 would also match the IPs 192.168.10-19 and 192.168.100-199. This result is probably unintended. The better solution would be to configure either:</p> <ul style="list-style-type: none"> a regular expression such as ^192.168.1.1\$ or a source IP condition instead of an HTTP header condition 	No default.
source-ip {address_ipv4 address_ipv6}	Type the IP address of a client that will be allowed. Depending on your configuration of how FortiWeb will derive the client's IP (see “waf x-forwarded-for” on page 413), this may be the IP address that is indicated in an HTTP header rather than the IP header.	No default.
request-file <url_str>	<p>Type a regular expression that defines either all matching or all non-matching URLs. Then, also configure reverse-match {yes no}.</p> <p>For example, for the URL access rule to match all URLs that begin with /wordpress, you could enter ^/wordpress, then, in reverse-match {yes no}, select no.</p> <p>The pattern is not required to begin with a slash (/). The maximum length is 255 characters.</p> <p>Note: Regular expressions beginning with an exclamation point (!) are not supported. Instead, use reverse-match {yes no}.</p>	No default.
reverse-match {no yes}	<p>Indicate how to use request-file <url_str> when determining whether or not this rule's condition has been met.</p> <ul style="list-style-type: none"> no — If the regular expression does match the request URL, the condition is met. yes — If the regular expression does not match the request URL, the condition is met. <p>The effect is equivalent to preceding a regular expression with an exclamation point (!).</p>	no
http-transaction-timeout <timeout_int>	<p>Specifies a timeout value of 1 to 3600 seconds.</p> <p>If the lifetime of a HTTP transaction exceeds this value, the transaction matches this condition.</p>	5

Variable	Description	Default
<response-code_int>	Specifies the start and end code in a range of HTTP response codes. To specify a single code, enter the same value for the start and end codes (for example, 404-404 or 500-503). If its HTTP response code is within this range, the HTTP transaction matches this condition.	No default.
packet-interval-timeout <timeout_int>	Specifies the maximum number of seconds allowed between packets arriving from either the client or server (request or response packets), in seconds. Enter a value from 1 to 60. If the interval exceeds this value, the HTTP transaction matches this condition.	1
{010000000 020000000 030000000 040000000 050000000 060000000 090000000}	Specifies the ID of a signature class. Ensure the signature is enabled in signature configuration before you use it in an advanced access control rule. See “waf signature” on page 355 .	No default.
status {enable disable}	Specifies whether the HTTP transaction matches this condition if it matches the specified signature.	disable
<occurrence_int>	Specifies the maximum number of times a transaction can match other filter types in the current rule during the time period specified by within. Enter a value between 1 and 100,000. If the number of matches exceeds this threshold, the associated HTTP source client IP address or client matches this condition.	1
<within_int>	Specifies the time period during which FortiWeb counts the number of times transactions match other filter types in the current rule. Enter a value between 1 and 600.	1
{Source-IP User}	Specifies whether FortiWeb determines the rate at which a transaction matches other filter types in the current rule by counting matches by source client IP address or by client. To specify user, ensure that the value of http-session-management is enabled (see “waf web-protection-profile inline-protection” on page 390).	source-ip

Example

This example allows access to URLs beginning with “/admin”, but only if they originate from 172.16.1.5, and only if the client does not exceed 5 requests per second.

Clients that violate this rule will be blocked for 60 seconds (the default duration). The violation will be logged in the attack log using `severity_level=High`, and all servers configured in `notification-servers1` will be used to notify the network administrator.

```
config waf custom-access rule
edit "combo-IP-rate-URL-rule1"
    set action block-period
    set severity High
    set trigger "notification-servers1"
```

```

config access-limit-filter
    edit 1
        set access-rate-limit 5
    next
end
config source-ip-filter
    edit 1
        set source-ip 172.16.1.5
    next
end
config url-filter
    edit 1
        set request-file "/admin*"
    next
end
next
end
config waf custom-access policy
    edit "combo-IP-rate-URL-policy1"
        config rule
            edit 1
                set rule-name "combo-access-rate-rule1"
            next
        end
    next
end

```

Related topics

- [config waf custom-access policy](#)
- [config log trigger-policy](#)
- [config waf signature](#)

waf custom-protection-group

Use this command to configure custom protection groups, creating sets of custom protection rules that can be used with attack signatures ("server protection rule").

Before you can configure this command, you must first define your custom data leak and attack signatures. For details, see ["config waf custom-protection-rule" on page 282](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config waf custom-protection-group
  edit <custom-protection group_name>
    config type-list
      edit <entry_index>
        set custom-protection-rule <rule_name>
      next
    end
  next
end
```

Variable	Description	Default
<custom-protection group_name>	Type the name of a new or existing group. The maximum length is 35 characters. To display the list of existing group, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
custom-protection-rule <rule_name>	Type the name of the custom protection rule to associate with the custom protection group. The maximum length is 35 characters. To display a list of the existing rules, type: set custom-protection-rule ?	No default.

Example

This example groups custom protection rule 1 and custom protection rule 3 together within Custom Protection group 1.

```
config waf custom-protection-group
  edit "Custom Protection group 1"
```



```
config type-list
  edit 1
    set custom-protection-rule "custom protection rule 3"
  next
  edit 3
    set custom-protection-rule "custom protection rule 1"
  next
end
next
end
```

Related topics

- [config waf signature](#)
- [config waf custom-protection-rule](#)

waf custom-protection-rule

Use this command to configure custom data leak and attack signatures.



Before you enter custom signatures via the CLI, first enable `cli-signature {enable | disable}` in `config system global`.

To use your custom signatures, you must first group them so that they can be included in a rule. For details, see “[config waf custom-protection-group](#)” on page 280.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “[Permissions](#)” on page 47.

Syntax

```
config waf custom-protection-rule
  edit <custom-protection rule_name>
    set type {request | response}
    set action {alert | alert_deny | alert_erase | redirect | block-
period | send_403_forbidden}
    set block-period <seconds_int>
    set case-sensitive {enable | disable}
    set expression <regex_pattern>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    config meet-targets
      edit <entry_index>
        set target {ARGS | ARGS_NAMES | REQUEST_BODY |
REQUEST_COOKIES | REQUEST_COOKIES_NAMES | REQUEST_FILENAME |
REQUEST_HEADERS | REQUEST_HEADERS_NAMES | REQUEST_RAW_URI |
REQUEST_URI | RESPONSE_HEADER | RESPONSE_BODY |
RESPONSE_STATUS}
      next
    end
  next
end
```

Variable	Description	Default
<custom-protection rule_name>	Type the name of the new or existing custom signature. The maximum length is 35 characters. To display a list of the existing rules, type: edit ?	No default.
type {request response}	Specify the type of regular expression: <ul style="list-style-type: none">request — The expression is an attack signature.data-leakage — The expression is a server information disclosure signature.	request

Variable	Description	Default
<pre>action {alert alert_deny alert_erase redirect block-period send_403_forbidden}</pre>	<p>Select the specific action to be taken when the request matches the this signature.</p> <ul style="list-style-type: none"> alert — Accept the request and generate an alert email and/or log message. Note: If type is data-leakage, does not cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) alert_deny — Block the request (or reset the connection) and generate an alert email and/or log message. This option is applicable only if type is signature-creation. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. alert_erase — Hide replies with sensitive information (sometimes called “cloaking”). Block the reply (or reset the connection) or remove the sensitive information, and generate an alert email and/or log message. This option is applicable only if type is data-leakage. If the sensitive information is a status code, you can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. Note: This option is not fully supported in offline protection mode. Effects will be identical to <code>alert</code>; sensitive information will not be blocked or erased. block-period — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. redirect — Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <code>redirect-url <redirect_fqdn></code> and <code>rdt-reason {enable disable}</code>. send_403_forbidden — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. This option is applicable only if type is signature-creation. 	alert

Variable	Description	Default
	<p>Caution: This setting will be ignored if monitor-mode {enable disable} is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	
<code>block-period <seconds_int></code>	<p>If action is <code>block-period</code>, number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule. For information on viewing the list of currently blocked clients, see the FortiWeb Administration Guide.</p> <p>The valid range is from 1 to 3,600 (1 hour).</p>	1
<code>case-sensitive {enable disable}</code>	<p>Enable to differentiate upper case and lower case letters when evaluating the web server’s response for data leaks according to expression <regex_pattern>.</p> <p>For example, when enabled, an HTTP reply containing the phrase <code>Credit card</code> would not match an expression that looks for the phrase <code>credit card</code> (difference highlighted in bold).</p>	enable
<code>expression <regex_pattern></code>	<p>Depending on your selection in type {request response}, type a regular expression that matches either:</p> <ul style="list-style-type: none"> an attack from a client a data leak from the server <p>To prevent false positives, it should not match anything else. The maximum length is 2,071 characters.</p>	No default.
<code>severity {High Medium Low}</code>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule.</p>	Medium
<code>trigger <trigger-policy_name></code>	<p>Select which trigger policy, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre>	No default.

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
target {ARGS ARGS_NAMES REQUEST_BODY REQUEST_COOKIES REQUEST_COOKIES_NAMES REQUEST_FILENAME REQUEST_HEADERS REQUEST_HEADERS_NAMES REQUEST_RAW_URI REQUEST_URI RESPONSE_HEADER RESPONSE_BODY RESPONSE_STATUS}	Type the name of a location in the HTTP request or response (for example, ARGS_NAMES for the names of parameters or REQUEST_COOKIES for strings in the HTTP Cookie: header) to scan for a signature match. If you want to scan multiple locations, create multiple entries in the meet-targets table.	No default.

Example

This example configures a signature to detect and block an LFI attack that uses directory traversal through an unsanitized `controller` parameter in older versions of Joomla. Each time it detects an attack, the trigger policy named `notification-servers1` will be used to send alert email and attack log messages whose severity level is `High`.

```
config waf custom-protection-rule
  edit "Joomla_controller_LFI"
    set type signature-creation
    set expression
      "^/index\.php\?option=com_ckforms\&controller=(\.\.\/)+?"
    set action alert_deny
    set severity High
    set trigger notification-servers1
    config meet-targets
      edit 1
        set target REQUEST_RAW_URI
      next
    end
  next
end
```

Related topics

- [config waf custom-protection-group](#)
- [config log trigger-policy](#)

waf exclude-url

Use this command to configure URLs that are exempt from a file compression or file decompression rule.

To apply an exclusion, include it in a compression or decompression rule. See [“config waf file-compress-rule” on page 288](#) or [“config waf file-uncompress-rule” on page 290](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf exclude-url
  edit <rule_name>
    config exclude-rules
      edit <entry_index>
        set host <protected-host_name>
        set host-status {enable | disable}
        set request-file <url_str>
      next
    end
  next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing exception. The maximum length is 35 characters. To display a list of the existing exceptions, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host <protected-host_name>	Type the name of a protected host that the <code>Host :</code> field of an HTTP request must be in order to match the exception. The maximum length is 255 characters. This setting applies only if <code>host-status</code> is <code>enable</code> .	No default.
host-status {enable disable}	Enable to apply this exception only to HTTP requests for specific web hosts. Also configure <code>host <protected-host_name></code> . Disable to match the exception based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	disable
request-file <url_str>	Type the literal URL, such as <code>/archives</code> , to which the exception applies. The URL must begin with a slash (<code>/</code>). Do not include the name of the host, such as <code>www.example.com</code> , which is configured separately using <code>host</code> . The maximum length is 255 characters.	No default.

Example

This example configures two exclusion rules, one for compression and the other for decompression. Either rule can be referenced by name in a file compression or file decompression rule.

```
config waf exclude-url
  edit "Compression Exclusion"
    config exclude-rules
      edit 1
        set host "192.168.1.2"
        set host-status enable
        set request-file "/archives"
      next
    end
  next
edit "Decompression Exclusion"
  config exclude-rules
    edit 1
      set host "www.example.com"
      set host-status enable
      set request-file "/products.cfm"
    next
  end
next
end
```

Related topics

- [config waf file-compress-rule](#)
- [config waf file-uncompress-rule](#)

waf file-compress-rule

Use this command to compress specific file types in HTTP replies.

Compression can reduce bandwidth, which can reduce delivery time to end users. Modern browsers automatically decompress files before they display web pages.

You can configure most web servers to compress files when they respond to a request. However, if you do not want to configure each of your web servers separately, or if you want to offload compression for performance reasons, you can configure FortiWeb to do the compression.

By default, the maximum pre-compressed file size is 64 KB. FortiWeb transmits files larger than the maximum without compression. You can use the `config system advanced` command's `max-cache-size` setting to adjust the maximum files size (see [“config system advanced” on page 175](#)).

To exclude specific URLs from compression, see [“config waf exclude-url” on page 286](#).

To apply a compression rule, select it in an inline protection profile. See [“config waf web-protection-profile inline-protection” on page 390](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf file-compress-rule
  edit <rule_name>
    config content-types
      edit <entry_index>
        set content-type <content-type_name>
      next
    end
    [set exclude-url <exclusion-rule_name>]
  next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
content-type <content-type_name>	<p>Type one of the following content types to compress it:</p> <ul style="list-style-type: none"> • text/plain • text/html • application/xml (or) text/xml • application/soap+xml • application/x-javascript • text/css • application/javascript • text/javascript <p>To compress multiple file types, add each file type in a separate table entry with its own <entry_index>. See “Example”.</p>	No default.
exclude-url <exclusion-rule_name>	Type the name of an exclusion to use with the rule, if any. See “config waf exclude-url” on page 286 . The maximum length is 35 characters.	No default.

Example

This example configures a file compression rule that compresses CSS and HTML files, unless they match one of the URLs in the exception named “Compression Exclusion 1”.

```
config waf file-compress-rule
  edit "Web Portal Compression Rule"
    config content-types
      edit 1
        set content-type text/css
      next
      edit 2
        set content-type text/html
      next
    end
    set exclude-url "Compression Exclusion 1"
  next
end
```

Related topics

- [config waf file-uncompress-rule](#)
- [config waf exclude-url](#)

waf file-uncompress-rule

Use this command to decompress a file that was already compressed by a protected web server.

Since the FortiWeb appliance cannot scan compressed files in order to perform features such as data leak prevention, you can configure the FortiWeb appliance to decompress files based on the file type.



By default, the maximum file size that FortiWeb can decompress is 64 KB. FortiWeb does not scan files larger than the maximum.

You can use the `config system advanced` command's `max-cache-size` setting to adjust the maximum files size (see [“config system advanced” on page 175](#)).



All decompressed files are recompressed after being scanned. As such, unlike [“waf file-compress-rule” on page 288](#), the effects of this command will not be visible to end-users.

To exclude specific URLs, see [“config waf exclude-url” on page 286](#).

To apply a decompression rule, select it in an inline or offline protection profile. See [“config waf web-protection-profile inline-protection” on page 390](#) or [“config waf web-protection-profile offline-protection” on page 406](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf file-uncompress-rule
  edit <rule_name>
    config content-types
      edit <entry_index>
        set content-type <content-type_name>
      next
    end
    [set exclude-url <exclusion-rule_name>]
  next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.

Variable	Description	Default
content-type <content-type_name>	<p>Specify one of the following content types:</p> <ul style="list-style-type: none"> • text/plain • text/html • application/xml (or) text/xml • application/soap+xml • application/x-javascript • text/css • application/javascript • text/javascript <p>To compress multiple file types, add each file type in a separate table entry with its own <entry_index>. See “Example”.</p>	No default.
exclude-url <exclusion-rule_name>	Type the name of an exclusion to use with the rule, if any. See “config waf exclude-url” on page 286 . The maximum length is 35 characters.	No default.

Example

The following example creates a decompression rule with two content types and one exclusion rule.

```
config waf file-uncompress-rule
  edit "Online Store Uncompress Rule"
    config content-types
      edit 1
        set content-type application/soap+xml
      next
      edit 2
        set content-type application/xml (or) text/xml
      next
    end
    set exclude-url "Uncompress Exclusion"
  next
end
```

Related topics

- [config waf file-compress-rule](#)
- [config waf exclude-url](#)

waf file-upload-restriction-policy

Use this command to set the file upload restriction policies that the FortiWeb appliance uses to limit the types of files that can be uploaded to your web servers.

The policies are composed of individual rules set using the [config waf file-upload-restriction-rule](#) command. Each rule identifies the host and/or URL to which the restriction applies and the types of files allowed. To apply a file upload restriction policy, select it within an inline or offline protection profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config waf file-upload-restriction-policy
edit <file-upload-restriction-policy_name>
    set action {alert | alert_deny | block-period}
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    set av-scan {enable |disable}
    set block-period <seconds_int>
config rule
    edit <entry_index>
        set file-upload-restriction-rule <rule_name>
    next
```

```

end
next
end

```

Variable	Description	Default
<file-upload-restriction-policy_name>	Type the name of an existing or new file upload restriction policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
action {alert alert_deny block-period}	Type the action you want FortiWeb to perform when the policy is violated: <ul style="list-style-type: none"> • alert — Accept the request and generate an alert and/or log message. • alert_deny — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the <i>FortiWeb Administration Guide</i> or <code>error-msg <message_str></code> in “server-policy policy” on page 140. • block-period — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled. Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64. Note: If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387. 	alert
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
trigger <trigger-policy_name>	Type the name of the trigger to apply when this policy is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing triggers, type: set trigger ?	No default.
av-scan {enable disable}	Specify <code>enable</code> to scan for trojans. Also enable and configure the signature rule for the Trojans class (0700000000; see “config waf signature” on page 355) .	

Variable	Description	Default
block-period <seconds_int>	If action is block-period, type the number of seconds that violating requests will be blocked. The valid range is from 1 to 3,600 seconds.	1
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
file-upload-restriction-rule <rule_name>	Type the name of an upload restriction rule to use with the policy, if any. See “config waf file-upload-restriction-rule” on page 295 . The maximum length is 35 characters. To display the list of existing rules, type: set file-upload-restriction-rule ?	No default.

Related topics

- [config waf file-upload-restriction-rule](#)
- [config log trigger-policy](#)

waf file-upload-restriction-rule

Use this command to define the specific host and request URL for which file upload restrictions apply, and define the specific file types that can be uploaded to that host or URL.

To apply the rule, select it in a file upload restriction policy. See [“config waf file-upload-restriction-policy” on page 292](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf file-upload-restriction-rule
edit <file-upload-restriction-rule_name>
    set host-status {enable | disable}
    set host <protected-host_name>
    set request-file <url_pattern>
    set request-type {regular | plain}
    [set file-size-limit <size_int>]
    config file-types
        edit <entry_index>
            set file-type-id <id_str>
            set file-type_name <file-type-extension_str>
        next
    end
next
end
```

Variable	Description	Default
<file-upload-restriction-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
host-status {enable disable}	Enable to apply this exception only to HTTP requests for specific web hosts. Also configure <code>host <protected-host_name></code> . Disable to match the exception based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	disable
host <protected-host_name>	Type the name of a protected host that the <code>Host :</code> field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting applies only if <code>host-status</code> is <code>enable</code> .	No default.

Variable	Description	Default
request-file <url_pattern>	<p>Depending on your selection in request-type {regular plain}, type either:</p> <ul style="list-style-type: none"> the literal URL, such as /fileupload, that the HTTP request must contain in order to match the signature exception. The URL must begin with a slash (/). a regular expression, such as ^/* .php, matching all and only the URLs to which the signature exception should apply. The pattern is not required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. <p>Do not include the name of the web host, such as www.example.com, which is configured separately in host <protected-host_name>. The maximum length is 255 characters.</p> <p>Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the FortiWeb Administration Guide.</p>	No default.
request-type {regular plain}	Select whether request-file <url_pattern> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
file-size-limit <size_int>	Optionally, enter a number to represent the maximum size in kilobytes for any individual file. This places a size limit on allowed file types. The valid range is from 0 to 5,120 KB (5 MB).	0
<entry_index>	Type the index number of the individual entry in the table. Each entry in the table can define one file type. The valid range is from 1 to 9,999,999,999,999,999.	No default.

Variable	Description	Default
file-type-id <id_str>	<p>Select the numeric type ID that corresponds to the file type. Recognized IDs are updated by FortiGuard services and may vary. For a list of available IDs, select all file types in the GUI, then use the CLI to view their corresponding IDs. Common IDs include:</p> <ul style="list-style-type: none"> • 00001 (GIF) • 00002 (JPG) • 00003 (PDF) • 00004 (XML) • 00005 (MP3) • 00006 (MIDI) • 00007 (WAVE) • 00008 (FLV for a Macromedia Flash Video) • 00009 (RAR) • 00010 (ZIP) • 00011 (BMP) • 00012 (RM for RealMedia) • 00013 (MPEG for MPEG v) • 00014 (3GPP) 	No default.
file-type_name <file-type-extension_str>	<p>Type the extension, such as MP3, of the file type to allow to be uploaded. Recognized file types are updated by FortiGuard services and may vary. For a list of available names, use the GUI.</p> <p>Note: Microsoft Office Open XML file types such as .docx, xlsx, .pptx, and .vsdx are a type of ZIP-compressed XML. If you specify restrictions for them, those signatures will take priority. However, if you do not select a MSOOX restriction but do have an XML or ZIP restriction, the XML and ZIP restrictions will still apply, and the files will still be restricted.</p>	No default.

Example

This example allows both MPEG and FLV files uploaded to the URL `/file-uploads` on the host `www.example.com`.

```
config waf file-upload-restriction-rule
edit file-upload-rule1
set host-status enable
set host www.example.com
set request-file /file-uploads
```

```
config file-types
  edit 1
    set file-type-id 00013
    set file-type-name MPEG
  next
  edit 2
    set file-type-id 00008
    set file-type-name FLV
  next
end
next
end
```

Related topics

- [config waf file-upload-restriction-policy](#)

waf geo-block-list

Use this command to define large sets of client IP addresses to block based upon their associated geographical location.



Because network mappings may change as networks grow and shrink, if you use this feature, be sure to periodically update the geography-to-IP mapping database. To download the file, go to the [Fortinet Technical Support web site](#).

Alternatively, you can block clients individually (see “[waf ip-list](#)” on page 336) or based upon their reputation (see “[waf ip-intelligence](#)” on page 332).

To apply the rule, select it in a protection profile. See “[config waf web-protection-profile inline-protection](#)” on page 390 or “[config waf web-protection-profile offline-protection](#)” on page 406.

To use this command, your administrator account’s access control profile must have either w or rw permission to the wafgrp area. For more information, see “[Permissions](#)” on page 47.

Syntax

```
config waf geo-block-list
  edit <geography-to-ip_name>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    config country-list
      edit <entry_index>
        set country-name "<region_name>"
      next
    end
  next
end
```

Variable	Description	Default
<geography-to-ip_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
trigger <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see “ config log trigger-policy ” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
country-name "<region_name>"	Type the name of a region (Antarctica or Bouvet Island) or country (U.S.) as it is written in English. Surround names with multiple words or apostrophes in double quotes. The list of locations varies by the currently installed IP-to-geography mapping package. For a current list of locations, use the web UI.	No default.

Example

This example creates a set of North American IP addresses that a server policy can use to block clients with IP addresses belonging to Belize and Canada.

```
config waf geo-block-list
  edit "north-america"
    set trigger "notification-servers1"
    set severity Low
    config country-list
      edit 1
        set country-name "Belize"
      next
      edit 2
        set country-name "Canada"
      next
    end
  next
end
```

Related topics

- [config log trigger-policy](#)
- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config waf ip-list](#)
- [config waf ip-intelligence](#)
- [diagnose debug flow trace](#)

waf hidden-fields-protection

Use this command to configure groups of hidden field rules.

To apply hidden field rule groups, select them within an inline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf hidden-fields-protection
  edit <hidden-field-group_name>
    config hidden_fields_list
      edit <entry_index>
        set hidden-field-rule <hidden-field-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
<hidden-field-group_name>	Type the name of a new or existing hidden field rule group. The maximum length is 35 characters. To display the list of existing groups, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
hidden-field-rule <hidden-field-rule_name>	Type the name of an existing hidden field rule to add to the group. The maximum length is 35 characters. To display the list of existing rules, type: set hidden-field-rule ?	No default.

Related topics

- [config waf hidden-fields-rule](#)
- [config waf web-protection-profile inline-protection](#)

waf hidden-fields-rule

Use this command to configure hidden field rules.

Hidden form inputs, like other types of parameters and inputs, can be vulnerable to tampering and can be used as a vector for other attacks.

Unlike other inputs, they are often written into an HTML page by the web server when it serves that page to the client, and are not visible on the rendered web page. As such, they are difficult for users to unintentionally modify, and are often incorrectly perceived as relatively safe by web site owners.

Like other inputs, however, they are accessible through the JavaScript document object model (DOM), and as inputs, can be used to inject invalid data into your databases or attempt to tamper with the session state.

Hidden field rules prevent such tampering. The FortiWeb appliance caches the values of a session's hidden inputs as they pass to the HTTP client, and verifies that they remain unchanged when the HTTP client submits a form.

You apply hidden field constraints by first grouping them into a hidden field group. For details, see [“config waf hidden-fields-protection” on page 301](#).

Before you configure a hidden field rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see [“config server-policy allow-hosts” on page 105](#).



Alternatively, you can use the web UI to fetch the request URL from the server and scan it for hidden inputs, using the results to configure the hidden input rule. For details, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf hidden-fields-rule
edit <hidden-field-rule_name>
    set action {alert | alert_deny | redirect | block-period |
    send_403_forbidden}
    set block-period <seconds_int>
    set host <protected-hosts_name>
    set host-status {enable | disable}
    set request-file <url_str>
    set action-url0 <url_str>
    set action-url1 <url_str>
    set action-url2 <url_str>
    set action-url3 <url_str>
    set action-url4 <url_str>
    set action-url5 <url_str>
    set action-url6 <url_str>
    set action-url7 <url_str>
    set action-url8 <url_str>
```

```
set action-url9 <url_str>
set severity {High | Medium | Low}
set trigger <trigger-policy_name>
config hidden-field-name
    edit <entry_index>
        set argument <hidden-field_str>
    next
```

```

end
next
end

```

Variable	Description	Default
<hidden-field-rule_name>	<p>Type the name of a new or existing rule. The maximum length is 35 characters.</p> <p>To display the list of existing rules, type:</p> <pre>edit ?</pre>	No default.
<pre>action {alert alert_deny redirect block-period send_403_forbidden}</pre>	<p>Select one of the following actions that the FortiWeb appliance will perform when an HTTP request violates one of the hidden field rules in the entry:</p> <ul style="list-style-type: none"> <code>alert</code> — Accept the request and generate an alert email and/or log message. <code>alert_deny</code> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. <code>block-period</code> — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. <code>redirect</code> — Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <code>redirect-url <redirect_fqdn></code> and <code>rdt-reason {enable disable}</code>. <code>send_403_forbidden</code> — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	alert
<pre>block-period <seconds_int></pre>	<p>If <code>action</code> is <code>block-period</code>, type the number of seconds that the connection will be blocked. The valid range is from 1 to 3,600 seconds.</p>	0

Variable	Description	Default
host <protected-hosts_name>	Type the name of a protected host that the Host : field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting applies only if host-status is enable.	No default.
host-status {enable disable}	Enable to apply this hidden field rule only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name> . Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the Host : field.	disable
request-file <url_str>	Type the literal URL, such as /login.jsp, that contains the hidden form. The URL must begin with a slash (/). Do not include the name of the web host, such as www.example.com, which is configured separately in host <protected-hosts_name> . Regular expressions are not supported. The maximum length is 255 characters.	No default.
action-url0 <url_str>	Add up to 10 URLs that are valid to use with the HTTP POST method when the client submits the form containing the hidden fields in this rule.	No default.
action-url1 <url_str>		
action-url2 <url_str>		
action-url3 <url_str>		
action-url4 <url_str>		
action-url5 <url_str>		
action-url6 <url_str>		
action-url7 <url_str>		
action-url8 <url_str>		
action-url9 <url_str>		
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	High
trigger <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
argument <hidden-field_str>	Type the name of the hidden form input, such as languagepref. The maximum length is 35 characters.	No default.

Example

This example blocks and logs requests from search.jsp if its hidden form input, whose name is “languagepref”, is posted to any URL other than query.do.

```
config waf hidden-fields-rule
edit "hidden_fields_rule1"
set action alert_deny
set request-file "/search.jsp"
set action-url0 "/query.do"
```

```
    config hidden-field-name
        edit 1
            set argument "languagepref"
        next
    end
next
end
```

Related topics

- [config server-policy allow-hosts](#)
- [config waf hidden-fields-protection](#)
- [config log trigger-policy](#)

waf http-authen http-authen-policy

Use this command to group HTTP authentication rules into HTTP authentication policies.

The FortiWeb appliance uses authentication policies with the HTTP authentication feature to authorize HTTP requests. For details, see the [FortiWeb Administration Guide](#).

To apply HTTP authentication policies, select them in an inline protection profile. For details, see “[config waf web-protection-profile inline-protection](#)” on page 390.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “[Permissions](#)” on page 47.

Syntax

```
config waf http-authen http-authen-policy
  edit <auth-policy_name>
    set cache {enable | disable}
    set alert-type {none | fail | success | all}
    set cache-timeout <timeout_int>
    set auth-timeout <timeout_int>
  config rule
    edit <entry_index>
      set http-authen-rule <http-auth-rule_name>
    next
  end
next
end
```

Variable	Description	Default
<auth-policy_name>	Type the name of a new or existing HTTP authentication policy. The maximum length is 35 characters. To display the list of existing policies, type: <code>edit ?</code>	No default.
cache {enable disable}	Enable to cache client user names and passwords from remote authentication such as LDAP queries. Also configure <code>cache-timeout <timeout_int></code> . This can be used can improve performance by preventing frequent queries.	No default.
alert-type {none fail success all}	Type the instances when alerts will be issued for HTTP authentication attempts: <ul style="list-style-type: none">• <code>none</code> — No alerts are issued for HTTP authentication.• <code>fail</code> — Alerts are issued only for HTTP authentication failures.• <code>success</code> — Alerts are issued for successful HTTP authentication.• <code>all</code> — Alerts are issued for all failed and successful HTTP authentication.	none
cache-timeout <timeout_int>	Type the query cache timeout, in seconds. The valid range is from 0 to 3,600 seconds. This option is available only when <code>cache</code> is enabled.	300

Variable	Description	Default
auth-timeout <timeout_int>	Type the connection timeout for the query to the FortiWeb's query to the remote authentication server in milliseconds. The valid range is from 0 to 60,000 milliseconds. If the authentication server does not answer queries quickly enough, to prevent dropped connections, increase this value.	2000
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
http-authen-rule <http-auth-rule_name>	Type the name of an existing HTTP authentication rule. The maximum length is 35 characters. To display the list of existing rules, type: set http-authen-rule ?	No default.

Example

This example first configures a user group that contains both a local user account and an LDAP query.

```
config user user-group
  edit "user-group1"
    config members
      edit 1
        set type local
        set local-name "user1"
      next
      edit 2
        set ldap-name "user2"
        set type ldap
      next
    end
  next
end
```

Second, it configures a rule that requires basic HTTP authentication when requesting the URL `/employees/holidays.html` on the host `www.example.com`. This URL will be identified as belonging to the realm named "Restricted Area". Users belonging to `user-group1` can authenticate.

```
config waf http-authen http-authen-rule
  edit "auth-rule1"
    set host-status enable
    set host "www.example.com"
    config rule
      edit 1
        set request-url "/employees/holidays.html"
        set authen-type basic
        set user-group "user-group1"
        set user-realm "Restricted Area"
      next
    end
  next
end
```

```
        end
    next
end
```

Third, it groups two HTTP authentication rules into an HTTP authentication policy that can be applied in an inline protection profile.

```
config waf http-authen http-authen-policy
    edit "http-auth-policy1"
        config rule
            edit 1
                set http-authen-rule "http-auth-rule1"
            next
            edit 2
                set http-authen-rule "http-auth-rule2"
            next
        end
    next
end
```

Related topics

- [config waf http-authen http-authen-rule](#)
- [config waf web-protection-profile inline-protection](#)

waf http-authen http-authen-rule

Use this command to configure HTTP authentication rules.

Authentication rules are used by the HTTP authentication feature to define sets of request URLs that will be authorized for each user group.

You apply authentication rules by adding them to an authentication policy, which is ultimately selected within an inline protection profile for use in web protection. For details, see [“config waf http-authen http-authen-policy” on page 307](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf http-authen http-authen-rule
  edit <auth-rule_name>
    set host <protected-hosts_name>
    set host-status {enable | disable}
    config rule
      edit <entry_index>
        set authen-type {basic | digest | ntlm}
        set request-url <path_str>
        set user-group <user-group_name>
        set user-realm <realm_str>
      next
    end
  next
end
```

Variable	Description	Default
<auth-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
host <protected-hosts_name>	Type the name of a protected host that the <code>Host :</code> field of an HTTP request must be in order to match the HTTP authentication rule. The maximum length is 255 characters. This setting applies only if <code>host-status</code> is <code>enable</code> .	No default.
host-status {enable disable}	Enable to apply this HTTP authentication rule only to HTTP requests for specific web hosts. Also configure <code>host <protected-hosts_name></code> . Disable to match the HTTP authentication rule based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	disable
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
<code>authen-type {basic digest ntlm}</code>	<p>Select which type of HTTP authentication to use, either:</p> <ul style="list-style-type: none"> <code>basic</code> — Clear text, Base64-encoded user name and password. Supports local user accounts, and RADIUS and LDAP user queries. NTLM user queries are not supported. <code>digest</code> — Hashed user name, realm, and password. RADIUS, LDAP and NTLM user queries are not supported. <code>ntlm</code> — Encrypted user name and password. Local user accounts and RADIUS and LDAP user queries are not supported. 	<code>basic</code>
<code>request-url <path_str></code>	Type the literal URL, such as <code>/employees/holidays.html</code> , that a request must match in order to trigger HTTP authentication. The maximum length is 255 characters.	No default.
<code>user-group <user-group_name></code>	<p>Type the name of a user group that is authorized to use the URL in request-url <path_str>. The maximum length is 35 characters.</p> <p>To display the list of existing user groups, type:</p> <pre>set user-group ?</pre>	No default.
<code>user-realm <realm_str></code>	<p>Type the realm, such as <code>Restricted Area</code>, to which the request-url <path_str> belongs. The maximum length is 35 characters.</p> <p>Browsers often use the realm multiple times.</p> <ul style="list-style-type: none"> It may appear in the browser's prompt for the user's credentials. Especially if a user has multiple logins, and only one login is valid for that specific realm, displaying the realm helps to indicate which user name and password should be supplied. After authenticating once, the browser may cache the authentication credentials for the duration of the browser session. If the user requests another URL from the same realm, the browser often will automatically re-supply the cached user name and password, rather than asking the user to enter them again for each request. <p>The realm may be the same for multiple authentication rules, if all of those URLs permit the same user group to authenticate.</p> <p>For example, the user group <code>All_Employees</code> could have access to the request-url <path_str> URLs <code>/wiki/Main</code> and <code>/wiki/ToDo</code>. These URLs both belong to the realm named <code>Intranet Wiki</code>. Because they use the same realm name, users authenticating to reach <code>/wiki/Main</code> usually will not have to authenticate again to reach <code>/wiki/ToDo</code>, as long as both requests are within the same browser session.</p> <p>This field does not appear if <code>authen-type</code> is <code>ntlm</code>, which does not support HTTP-style realms.</p>	No default.

Example

For an example, see [“config waf http-authen http-authen-policy” on page 307](#).

Related topics

- [config user user-group](#)
- [config waf http-authen http-authen-policy](#)

waf http-connection-flood-check-rule

Use this command to limit the number of TCP connections per HTTP session. This can prevent TCP connection floods from clients operating behind a shared IP with innocent clients.

Excessive numbers of TCP connections per session can occur if a web application or client is malfunctioning, or if an attacker is attempting to waste socket resources to produce a DoS.

This feature is similar to [config waf layer4-connection-flood-check-rule](#). However, this feature counts TCP connections per session cookie, while TCP flood prevention counts only TCP connections per IP address. Because it uses session cookies at the application layer instead of only TCP/IP connections at the network layer, this feature can differentiate multiple clients that may be behind the same source IP address, such as when the source IP address hides a subnet that uses network address translation (NAT). However, in order to work, the client must support cookies.

To apply this rule, include it in an application-layer DoS-prevention policy. See [“config waf application-layer-dos-prevention” on page 265](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf http-connection-flood-check-rule
edit <rule_name>
    set action {alert | alert_deny | block-period}
    set block-period <seconds_int>
    set http-connection-threshold <limit_int>
    set severity {High | Medium | Low}
```

```

set trigger-policy <trigger-policy_name>
next
end

```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
action {alert alert_deny block-period}	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the rate limit: <ul style="list-style-type: none"> alert — Accept the connection and generate an alert email and/or log message. alert_deny — Block the connection and generate an alert email and/or log message. block-period — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	alert
block-period <seconds_int>	Type the length of time for which the FortiWeb appliance will block additional requests after a client exceeds the rate threshold. The valid range is from 1 to 3,600 seconds.	1
http-connection-threshold <limit_int>	Type the maximum number of TCP connections allowed from the same client. The valid range is from 1 to 1,024.	1
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
trigger-policy <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see “ config log trigger-policy ” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.

Related topics

- [config log trigger-policy](#)
- [config waf application-layer-dos-prevention](#)

waf http-constraints-exceptions

Use set statements under this command to configure exceptions to existing HTTP protocol parameter constraints for specific hosts.

Exceptions may be useful if you know that some HTTP protocol constraints, during normal use, will cause false positives by matching an attack signature. Exceptions define HTTP constraints that will **not** be subject to HTTP protocol constraint policy.

For example, if you enable `max-http-header-length` in a HTTP protocol constraint exception for a specific host, FortiWeb ignores the HTTP header length check when executing the web protection profile for that host.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf http-constraints-exceptions
edit <http-exception_name>
  config http_constraints-exception-list
  edit <entry_index>
    set request-file <url_pattern>
    set request-type {plain | regular}
    set host <protected-hosts_name>
    set host-status {enable | disable}
    set block-malformed-request {enable | disable}
    set Illegal-host-name-check {enable | disable}
    set Illegal-http-request-method-check {enable | disable}
    set max-cookie-in-request {enable | disable}
    set max-header-line-request {enable | disable}
    set max-http-body-length {enable | disable}
    set max-http-content-length {enable | disable}
    set max-http-header-length {enable | disable}
    set max-http-header-line-length {enable | disable}
    set max-http-parameter-length {enable | disable}
    set max-http-request-length {enable | disable}
    set max-url-parameter {enable | disable}
    set max-url-parameter-length {enable | disable}
    set number-of-ranges-in-range-header {enable | disable}
  next
end
```

next
end

Variable	Description	Default
<http-exception_name>	Type the name of a new or existing HTTP protocol constraint exception. The maximum length is 35 characters. To display the list of existing exceptions, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
request-file <url_pattern>	Type either: <ul style="list-style-type: none"> the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a slash (/). a regular expression, such as ^/* .php, matching all and only the URLs to which the input rule should apply. The pattern is not required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. Do not include the name of the web host, such as www.example.com, which is configured separately in host. The maximum length is 255 characters.	No default.
request-type {plain regular}	Type either plain or regular (for a regular expression) to match the string entered in request-file.	No default.
host <protected-hosts_name>	Type the name of a protected host that the Host : field of an HTTP request must be in order to match the exception. The maximum length is 255 characters. This setting applies only if host-status is enable.	No default.
host-status {enable disable}	Enable to apply this exception only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name> . Disable to match the exception based upon the other criteria, such as the URL, but regardless of the Host : field.	disable
block-malformed-request {enable disable}	Enable to omit the constraint on syntax and FortiWeb parsing errors. Caution: Some web applications require abnormal or very large HTTP POST requests. Since allowing such errors and excesses is generally bad practice and can lead to vulnerabilities, use this option to omit the malformed request scan only if absolutely necessary.	
Illegal-host-name-check {enable disable}	Enable to omit the constraint on host names with illegal characters.	disable
Illegal-http-request-method-check {enable disable}	Enable to omit the constraint on illegal HTTP request methods.	disable
max-cookie-in-request {enable disable}	Enable to omit the constraint on the maximum number of cookies per request.	disable
max-header-line-request {enable disable}	Enable to omit the constraint on the maximum number of HTTP header lines.	disable
max-http-body-length {enable disable}	Enable to omit the constraint on the maximum HTTP body length.	disable
max-http-content-length {enable disable}	Enable to omit the constraint on the maximum HTTP content length.	disable

Variable	Description	Default
max-http-header-length {enable disable}	Enable to omit the constraint on the maximum HTTP header length.	disable
max-http-header-line-length {enable disable}	Enable to omit the constraint on the maximum HTTP header line length.	disable
max-http-parameter-length {enable disable}	Enable to omit the constraint on the maximum HTTP parameter length.	disable
max-http-request-length {enable disable}	Enable to omit the constraint on the maximum HTTP request length.	disable
max-url-parameter {enable disable}	Enable to omit the constraint on the maximum number of parameters in the URL.	disable
max-url-parameter-length {enable disable}	Enable to omit the constraint on the maximum length of parameters in the URL.	disable
number-of-ranges-in-range-header {enable disable}	Enable to omit the constraint on the maximum acceptable number of Range: fields of an HTTP header.	disable

Example

This example omits header length limits for HTTP requests to www.example.com and 10.0.0.1 for /login.asp.

```
config waf http-constraints-exceptions
edit "exception1"
  config http_constraints-exception-list
  edit 1
    set host "www.example.com"
    set host-status enable
    set max-http-header-length enable
    set request-file "/login.asp"
  next
  edit 2
    set host "10.0.0.1"
    set host-status enable
    set max-http-body-length enable
    set request-file "/login.asp"
  next
end
next
end
```

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config log trigger-policy](#)
- [config waf http-protocol-parameter-restriction](#)

waf http-protocol-parameter-restriction

Use this command to configure HTTP protocol constraints.

HTTP constraints govern features such as the HTTP header fields in the protocol itself, as well as the length of the HTML, XML, or other documents or encapsulated protocols carried in the content payload.

Use protocol constraints to prevent attacks such as buffer overflows in web servers that do not restrict elements of the HTTP protocol to acceptable lengths, or mishandle malformed requests. Such errors can lead to security vulnerabilities.



You can also use protocol constraints to block requests that are too large for the memory size you have configured for FortiWeb's scan buffers. If your web applications do not require large HTTP POST requests, configure [“block-malformed-request-check {enable | disable}”](#) on [page 320](#) to harden your configuration. To configure the buffer size, see [“max-http-argbuf-length {8k-cache | 12k-cache | 32k-cache | 64k-cache}”](#) on [page 176](#).

Each protocol parameter can be uniquely configured with an action, severity and trigger that determines how an attack on that parameter is handled. For example, header constraints could have the action set to alert, the severity set to high, and a trigger set to deliver an email each time these protocol parameters are violated.

To apply HTTP protocol constraints, select them in an inline or offline protection profile. For details, see [“config waf web-protection-profile inline-protection”](#) on [page 390](#) or [“config waf web-protection-profile offline-protection”](#) on [page 406](#).

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see [“Permissions”](#) on [page 47](#).

Syntax

```
config waf http-protocol-parameter-restriction
edit <http_constraint_name>
    set block-malformed-request-check {enable | disable}
    set Illegal-host-name-check {enable | disable}
    set Illegal-http-request-method-check {enable | disable}
    set Illegal-http-version-check {enable | disable}
    set max-cookie-in-request <limit_int>
    set max-header-line-request <limit_int>
    set max-http-body-length <limit_int>
    set max-http-content-length <limit_int>
    set max-http-header-length <limit_int>
    set max-http-header-line-length <limit_int>
    set max-http-parameter-length <limit_int>
    set max-http-request-length <limit_int>
    set max-url-parameter <limit_int>
    set max-url-parameter-length <limit_int>
    set number-of-ranges-in-range-header <limit_int>
    set <parameter_name>-action {alert | alert_deny | block-period}
    set <parameter_name>-severity {High | Medium | Low}
    set <parameter_name>-trigger <trigger-policy_name>
    set <parameter_name>-block-period <seconds_int>
```

```

[set exception_name <http-exception_name>]
next
end

```

Variable	Description	Default
<http-constraint_name>	Type the name of a new or existing HTTP protocol constraint. The maximum length is 35 characters. To display the list of existing constraints, type: edit ?	No default.
block-malformed-request-check {enable disable}	<p>Enable to block the request if either:</p> <ul style="list-style-type: none"> it has syntax errors parsing errors occur while FortiWeb is scanning the request (see “debug flow trace” on page 455) <p>These can cause problems in web servers that do not handle them gracefully. Such problems can lead to security vulnerabilities.</p> <p>Caution: Fortinet strongly recommends to enable this option <i>unless</i> large requests or parameters are required by the web application. If part of a request is too large for its scan buffer, FortiWeb cannot scan it for attacks. <i>Unless you enable this option to block oversized items, FortiWeb will allow oversized those requests to pass through without scanning.</i> This could allow attackers to craft large attacks to bypass your FortiWeb policies, and reach your web servers. If feasible, instead of disabling this option:</p> <ul style="list-style-type: none"> enlarge the scan buffers (see “max-http-argbuf-length {8k-cache 12k-cache 32k-cache 64k-cache}” on page 176) omit this only for URLs that require oversized parameters (see “config waf http-constraints-exceptions” on page 315) <p>Note: Do <i>not</i> enable this option if requests normally contain:</p> <ul style="list-style-type: none"> parameters larger than the scan buffer (Buffer size is configurable — see “max-http-argbuf-length {8k-cache 12k-cache 32k-cache 64k-cache}” on page 176.) large numbers of parameters more than 32 cookies <p>Requests like this will be flagged as potentially malformed by FortiWeb’s parser, causing FortiWeb to block normal requests.</p>	enable
Illegal-host-name-check {enable disable}	Enable to check the Host : line of the HTTP header for illegal characters, such as null or encoded characters like 0x0 or %00*.	enable
Illegal-http-request-method-check {enable disable}	Enable to check for illegal HTTP version numbers.	enable
Illegal-http-version-check {enable disable}	Enable to check for illegal HTTP version numbers. If the HTTP version is not “HTTP/1.0” or “HTTP/1.1”, it is considered illegal.	enable
max-cookie-in-request <limit_int>	Type the maximum acceptable number of cookies in an HTTP request. The valid range is from 0 to 32.	16
max-header-line-request <limit_int>	Type the maximum acceptable number of lines in the HTTP header. The valid range is from 0 to 32.	32

Variable	Description	Default
max-http-body-length <limit_int>	Type the maximum acceptable length in bytes of the HTTP body. The valid range is from 0 to 67,108,864. To disable the limit, type 0.	0
max-http-content-length <limit_int>	Type the maximum acceptable length in bytes of the request body. Length is determined by comparing this limit with the value of the Content-Length: field in the HTTP header. The valid range is from 0 to 67,108,864. To disable the limit, type 0.	0
max-http-header-length <limit_int>	Type the maximum acceptable length in bytes of the HTTP header. The valid range is from 0 to 12,288. To disable the limit, type 0.	4096
max-http-header-line-length <limit_int>	Type the maximum acceptable length in bytes of each line in the HTTP header. The valid range is from 0 to 12,288. To disable the limit, type 0.	1024
max-http-parameter-length <limit_int>	Type the total maximum total acceptable length in bytes of all parameters in the URL and/or, for HTTP POST requests, the HTTP body. Question mark (?), ampersand (&), and equal (=) characters are not included. The valid range is from 0 to 65,536. To disable the limit, type 0.	6144
max-http-request-length <limit_int>	Type the maximum acceptable length in bytes of the HTTP request. The valid range is from 0 to 67,108,864. To disable the limit, type 0.	67108864
max-url-parameter <limit_int>	Type the maximum number of URL parameters. The valid range is from 1 to 64.	16
max-url-parameter-length <limit_int>	Type the total maximum acceptable length in bytes of all parameters, including their names and values, in the URL. Parameters usually appear after a ?, such as: /url?parameter=value It does not include parameters in the HTTP body, which can occur with HTTP POST requests. The valid range is from 0 to 12,288.	2048
number-of-ranges-in-range-header <limit_int>	Type the maximum acceptable number of Range: fields of an HTTP header. Tip: Some versions of Apache are vulnerable to a denial of service (DoS) attack on this header, where a malicious client floods the server with many Range: headers. The default value is appropriate for unpatched versions of Apache 2.0 and 2.1. The valid range is from 0 to 64.	5

Variable	Description	Default
<code><parameter_name>-action {alert alert_deny block-period}</code>	<p>Select one of the following actions that the FortiWeb appliance will perform when an HTTP request violates one of the rules:</p> <ul style="list-style-type: none"> • <code>alert</code> — Accept the request and generate an alert email and/or log message. • <code>alert_deny</code> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. • <code>block-period</code> — Block subsequent requests from the client for a number of seconds. Also configure <code><parameter_name>-block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you <i>must</i> also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block <i>all</i> connections when it detects a violation of this type. <p>Caution: This setting is ignored when the value of <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p> <p>Note: This is not a single setting. Configure the action setting for each violation type. The number of action settings equals the number of violation types. For example, for maximum HTTP header length violations, you might type the accompanying setting:</p> <pre>set max-http-header-length-action alert</pre> <p>Note: Available actions vary depending on operating mode and protocol parameter.</p>	alert
<code><parameter_name>-severity {High Medium Low}</code>	<p>Select the severity level to use in logs and reports generated when a violation of the rule occurs.</p> <p>Note: This is not a single setting. Configure the severity setting for each violation type. The number of severity settings equals the number of violation types. For example, for maximum HTTP header length violations, you might type the accompanying setting:</p> <pre>set max-http-header-length-severity High</pre>	High

Variable	Description	Default
<code><parameter_name>-trigger <trigger-policy_name></code>	<p>Type the name of the trigger to apply when this rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre> <p>Note: This is not a single setting. Configure the trigger setting for each violation type. The number of trigger settings equals the number of violation types.</p> <p>For example, for maximum HTTP header length violations, you might type accompanying setting:</p> <pre>set max-http-header-length-trigger trigger-policy1</pre>	No default.
<code><parameter_name>-block-period <seconds_int></code>	If action is <code>block-period</code> , type the number of seconds that the connection will be blocked. The valid range is from 1 to 3,600 seconds.	0
<code>exception_name <http-exception_name></code>	Type the name of an exceptions to existing HTTP protocol parameter constraints (see “config waf http-constraints-exceptions” on page 315).	

Example

This example limits the total size of the HTTP header, including all lines, to 2,048 bytes. If the HTTP header length exceeds 2,048 bytes, the FortiWeb appliance takes an action to create a log message (`alert`), identifying the violation as `medium` severity, and sends an email to the administrators defined within the trigger policy `email-admin`.

```
config waf http-protocol-parameter-restriction
  edit "http-constraint1"
    set max-http-header-length 2048
    set max-http-header-length-action alert
    set max-http-header-length-severity Medium
    set max-http-header-length-trigger email-admin
  next
end
```

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config log trigger-policy](#)
- [config waf http-constraints-exceptions](#)
- [diagnose debug application http](#)
- [diagnose debug flow trace](#)

waf http-request-flood-prevention-rule

Use this command to limit the maximum number of HTTP requests per second coming from any client to a specific URL on one of your protected servers.

The FortiWeb appliance tracks the requests using a session cookie. If the count exceeds the request limit, FortiWeb performs the specified action.

To apply this rule, include it in an application-layer DoS-prevention policy. This feature is effective only when `http-session-management` is enabled in the inline protection profile that uses the parent DoS-prevention policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf http-request-flood-prevention-rule
  edit <rule_name>
    set access-limit-in-http-session <limit_int>
    set action {alert | alert_deny | block-period}
    set real-browser-enforcement {enable | disable}
    set block-period <seconds_int>
    set severity {High | Medium | Low}
    set trigger-policy <trigger-policy_name>
  next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
access-limit-in-http-session <limit_int>	Type the maximum number of HTTP connections allowed per second from the same client. The valid range is from 0 to 4,096.	0

Variable	Description	Default
action {alert alert_deny block-period}	<p>Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the limit:</p> <ul style="list-style-type: none"> alert — Accept the request and generate an alert email and/or log message. alert_deny — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. block-period — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	alert
real-browser-enforcement {enable disable}	<p>Enable to return a JavaScript to the client to test whether it is a web browser or automated tool when it exceeds the rate limit.</p> <p>If the client either fails the test or does not return results before the timeout specified by <code>validation-timeout</code>, FortiWeb applies the specified action. If the client appears to be a web browser, FortiWeb allows the client to exceed the rate limit.</p> <p>Disable this option to apply the rate limit regardless of whether the client is a web browser (for example, Firefox) or an automated tool (for example, wget).</p>	disable
block-period <seconds_int>	<p>If action is block-period, type the number of seconds that the connection will be blocked.</p> <p>This setting applies only if action is block-period. The valid is from 0 to 10,000 seconds.</p>	0
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium

Variable	Description	Default
trigger-policy <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
validation-timeout <timeout_int>	Specifies the maximum amount of time that FortiWeb waits for results from the client for Real Browser Enforcement.	

Example

This example illustrates a rule that imposes a two-minute blocking period on clients that exceed the set request limit.

```
config waf http-request-flood-prevention-rule
  edit "Web Portal HTTP Request Limit"
    set access-limit-in-http-session 10
    set action block-period
    set block-period 120
    set severity Medium
    set trigger-policy "Server_Policy_Trigger"
  next
end
```

Related topics

- [config log trigger-policy](#)
- [config waf application-layer-dos-prevention](#)

waf input-rule

Use this command to configure input rules.

Input rules define whether or not parameters are required, and sets their maximum allowed length, for HTTP requests matching the host and URL defined in the input rule.

Each input rule contains one or more individual rules. This enables you to define, within one input rule, all parameter restrictions that apply to HTTP requests matching that URL and host name.

For example, one web page might have multiple inputs: a user name, password, and a preference for whether or not to remember the login. Within the input rule for that web page, you could define separate rules for each parameter in the HTTP request: one rule for the user name parameter, one rule for the password parameter, and one rule for the preference parameter.

To apply input rules, select them within a parameter validation rule. For details, see [“config waf parameter-validation-rule” on page 353](#).

Before you configure an input rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see [“config server-policy allow-hosts” on page 105](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf input-rule
edit <input-rule_name>
    set action {alert | alert_deny | redirect | send_403_forbidden |
    block-period}
    set block-period <seconds_int>
    set host <protected-host_name>
    set host-status {enable | disable}
    set request-file <url_str>
    set request-type {plain | regular}
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
config rule-list
    edit <entry_index>
        set type-checked {enable | disable}
        set argument-type <custom-data-type | data-type | regular-
        expression>
        set argument-name <input_name>
        set argument-expression <regex_pattern>
        set custom-data-type <custom-data-type_name>
        set data-type <predefined_name>
        set is-essential {yes | no}
        set max-length <limit_int>
    next
end
```

```

next
end

```

Variable	Description	Default
<code><input-rule_name></code>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
<code>action {alert alert_deny redirect send_403_forbidden block-period}</code>	Select one of the following actions that the FortiWeb appliance will perform when an HTTP request violates one of the input rules in the entry: <ul style="list-style-type: none"> <code>alert</code> — Accept the request and generate an alert email and/or log message. <code>alert_deny</code> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. <code>block-period</code> — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. <code>redirect</code> — Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <code>redirect-url <redirect_fqdn></code> and <code>rdt-reason {enable disable}</code>. <code>send_403_forbidden</code> — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	<code>alert</code>
<code>block-period <seconds_int></code>	Type the number of seconds to block the source IP. The valid range is from 0 to 3,600 seconds. This setting applies only if <code>action</code> is <code>block-period</code> .	60
<code>host <protected-host_name></code>	Type the name of a protected host that the <code>Host :</code> field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting applies only if <code>host-status</code> is <code>enable</code> .	No default.

Variable	Description	Default
host-status {enable disable}	<p>Enable to apply this input rule only to HTTP requests for specific web hosts. Also configure host <protected-host_name>.</p> <p>Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the Host : field.</p>	disable
request-file <url_str>	<p>Depending on your selection in request-type {plain regular}, type either:</p> <ul style="list-style-type: none"> the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a slash (/). a regular expression, such as ^/* .php, matching all and only the URLs to which the input rule should apply. The pattern is not required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. <p>Do not include the name of the web host, such as www.example.com, which is configured separately in host <protected-host_name>. The maximum length is 255 characters.</p> <p>Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the FortiWeb Administration Guide.</p>	No default.
request-type {plain regular}	Select whether request-file <url_str> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
trigger <trigger-policy_name>	<p>Type the name of the trigger to apply when this rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
is-essential {yes no}	Select yes if the parameter is required for HTTP requests to this combination of Host : field and URL. Otherwise, select no.	no
max-length <limit_int>	<p>Type the maximum allowed length of the parameter value.</p> <p>The valid range is from 0 to 1,024 characters. To disable the length limit, type 0.</p>	0
type-checked (enable disable)	<p>Enable to use predefined or configured data types when validating parameters. Also configure data-type, custom-data-type, or argument-expression.</p> <p>Disable to ignore data-type and custom-data-type settings.</p>	enable

Variable	Description	Default
argument-type <custom-data-type data-type regular-expression>	Specify the type of argument.	No default.
argument-name <input_name>	Type the name of the input as it appears in the HTTP content, such as <code>username</code> . The maximum length is 35 characters.	No default.
argument-expression <regex_pattern>	Type a regular expression that matches all valid values, and no invalid values, for this input. The maximum length is 2,071 characters. Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported.	
custom-data-type <custom-data-type_name>	Type the name of a custom data type, if any. The maximum length is 35 characters. To display the list of custom data types, type: <code>set custom-data-type ?</code> This setting applies only if <code>type-checked</code> is enable.	No default.
data-type <predefined_name>	Select one of the predefined data types, if the input matches one of them (available options vary by FortiGuard updates). To display available options, type: <code>set data type ?</code> For match descriptions of each option, see “server-policy pattern data-type-group” on page 130). Alternatively, configure argument-type <custom-data-type data-type regular-expression> . This option is ignored if you configure argument-type <custom-data-type data-type regular-expression> , which also defines parameters to which the input rule applies, but supersedes this option.	No default.

Example

This example blocks and logs requests for the file named `login.php` that do not include a user name and password, both of which are required, or whose user name and password exceed the 64-character limit.

```
config waf input-rule
  edit "input_rule1"
    set action alert_deny
    set request-file "/login.php?*"
    request-type regular
```

```
config rule-list
  edit 1
    set argument-name "username"
    set argument-type data-type
    set data-type Email
    set is-essential yes
    set max-length 64
  next
  edit 2
    set argument-name "password"
    set data-type String
    set is-essential yes
    set max-length 64
  next
end
next
end
```

Related topics

- [config server-policy allow-hosts](#)
- [config waf parameter-validation-rule](#)

waf ip-intelligence

Use this command to configure reputation-based source IP blacklisting.

Clients with suspicious behaviors or poor reputations include spammers, phishers, botnets, and anonymizing proxy users. If you have purchased a subscription for the FortiGuard IP Reputation service, your FortiWeb can periodically download an updated blacklist to keep your appliance current with changes in dynamic IPs, spreading virus infections, and spammers changing service providers.

IP intelligence settings apply globally, to all policies that use this feature.

Before or after using this command, configure any exemptions that you want to apply by using the command [“waf ip-intelligence-exception” on page 335](#). To apply IP reputation-based blocking, configuring these category settings first, then enable `ip-intelligence {enable | disable}` in the server policy’s protection profile.

Alternatively, you can block sets of many clients based upon their geographical origin (see [“waf geo-block-list” on page 299](#)) or manually by specific IPs (see [“waf ip-list” on page 336](#)).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf ip-intelligence
edit <entry_index>
    set action {alert | alert_deny | redirect | send_403_forbidden |
    block-period}
    set block-period <seconds_int>
    set category <category_name>
    set severity {Low | Medium | High}
    set status {enable | disable}
```

```

set trigger <trigger-policy_name>
next
end

```

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table entry in the table.	No default.
action {alert alert_deny redirect send_403_forbidden block-period}	<p>Select one of the following actions that the FortiWeb appliance performs when a client's source IP matches the blacklist category:</p> <ul style="list-style-type: none"> • alert — Accept the request and generate an alert email and/or log message. • alert_deny — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. • block-period — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. • redirect — Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <code>redirect-url <redirect_fqdn></code> and <code>rdt-reason {enable disable}</code>. • send_403_forbidden — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. <p>Caution: FortiWeb ignores this setting when <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select alert. If the action is <code>alert_deny</code>, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	alert
block-period <seconds_int>	<p>Type the number of seconds to block the source IP. The valid range is from 0 to 3,600 seconds.</p> <p>This setting applies only if action is <code>block-period</code>.</p>	60
category <category_name>	<p>Type the name of an existing IP intelligence category, such as "Anonymous Proxy" or Botnet. If the category name contains a space, you must surround the name in double quotes. The maximum length is 35 characters.</p> <p>Category names vary by the version number of your FortiGuard IRIS package.</p>	
status {enable disable}	Enable to block clients whose source IP belongs to this category according to the FortiGuard IRIS service.	enable

Variable	Description	Default
severity {Low Medium High}	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance uses when a blacklisted IP address attempts to connect to your web servers:</p> <ul style="list-style-type: none"> • Low • Medium • High 	Low
trigger <trigger-policy_name>	<p>Select which trigger, if any, that the FortiWeb appliance uses when it logs and/or sends an alert email about a blacklisted IP address's attempt to connect to your web servers (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre>	No default.

Example

The following command blacklists clients whose source IPs are currently known by Fortinet to be members of a botnet. In the FortiGuard IRIS package for this example, “Botnet” is the first item in the list of categories.

When a botnet member makes a request, FortiWeb blocks the connection and continues to block it without re-evaluating it for the next 6 minutes (360 seconds). FortiWeb logs the event with a high severity level and sends notifications to the Syslog and email servers specified in `notification-servers1`.

```
config waf ip-intelligence
  edit 1
    set status enable
    set action period_block
    set block-period 360
    set severity High
    set trigger-policy notification-servers1
  next
end
```

Related topics

- [config waf ip-intelligence-exception](#)
- [config log trigger-policy](#)
- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config waf geo-block-list](#)
- [config waf ip-list](#)
- [diagnose debug flow trace](#)

waf ip-intelligence-exception

Use this command to exempt IP addresses from reputation-based blocking. The settings apply globally, to all policies that use this feature.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf ip-intelligence-exception
  edit <entry_index>
    set status {enable | disable}
    set ip <client_ipv4>
  next
end
```

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
status {enable disable}	Enable to exempt clients from IP reputation-based blocking.	disable
ip <client_ipv4>	Type the client's source IP address.	No default.

Example

See [“config waf ip-intelligence” on page 332](#).

Related topics

- [config waf ip-intelligence](#)

waf ip-list

Use this command to define which source IP addresses are trusted clients, undetermined, or distrusted.

- **Trusted IPs** — Almost always allowed to access to your protected web servers. Trusted IPs are exempt from many (but not all) of the restrictions that would otherwise be applied by a server policy. To determine skipped scans, see [“debug flow trace” on page 455](#).
- **Neither** — If a source IP address *is neither* explicitly blacklisted or trusted by an IP list policy, the client can access your web servers, *unless* it is blocked by any of your other configured, subsequent web protection scan techniques (see [“debug flow trace” on page 455](#)).
- **Blacklisted IPs** — Blocked and prevented from accessing your protected web servers. Requests from blacklisted IP addresses receive a warning message in response. The warning message page includes *ID: 70007*, which is the ID of all attack log messages about requests from blacklisted IPs.



Because FortiWeb evaluates trusted and blacklisted IP policies before many other techniques, defining these IP addresses can improve performance.

Alternatively, you can block sets of many clients based upon their reputation (see [“waf ip-intelligence” on page 332](#)) or geographical origin (see [“waf geo-block-list” on page 299](#)).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf ip-list
  edit <ip-list_name>
    config members
      edit <entry_index>
        set ip <client_ip>
        set type {trust-ip | black-ip}
        set severity {Low | Medium | High}
        set trigger-policy <trigger-policy_name>
      next
    end
  next
end
```

Variable	Description	Default
<ip-list_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual entry in the table entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.

Variable	Description	Default
ip <client_ip>	<p>Enter one of the following values:</p> <ul style="list-style-type: none"> • A single IP address that a client source IP must match, such as a trusted private network IP address (e.g. an administrator's computer, 172.16.1.20). • A range or addresses (for example, 172.22.14.1-172.22.14.255 or 10:200::10:1-10:200:10:100). 	No default.
type {trust-ip black-ip}	<p>Select either:</p> <ul style="list-style-type: none"> • trust-ip — The source IP address is trusted and allowed to access your web servers, unless it fails a previous scan (see “debug flow trace” on page 455). • black-ip — The source IP address that is distrusted, and is permanently blocked (blacklisted) from accessing your web servers, even if it would normally pass all other scans. <p>Note: If multiple clients share the same source IP address, such as when a group of clients is behind a firewall or router performing network address translation (NAT), blacklisting the source IP address could block innocent clients that share the same source IP address with an offending client.</p>	trust-ip
severity {Low Medium High}	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (severity_level) field. Select which severity level the FortiWeb appliance will use when a blacklisted IP address attempts to connect to your web servers:</p> <ul style="list-style-type: none"> • Low • Medium • High 	No default.
trigger-policy <trigger-policy_name>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a blacklisted IP address's attempt to connect to your web servers (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre>	No default.

Example

The following shows the configuration for a trusted host of 192.0.2.0 followed by a blacklisted client of 192.0.2.1.

```
config waf ip-list
  edit "IP-List-Policy1"
```

```
config members
  edit 1
    set ip 192.0.2.0
  next
  edit 2
    set type black-ip
    set ip 192.0.2.1
    set severity Medium
    set trigger-policy "TriggerActionPolicy1"
  next
end
next
end
```

Related topics

- [config log trigger-policy](#)
- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config waf geo-block-list](#)
- [config waf ip-intelligence](#)
- [diagnose debug flow trace](#)

waf layer4-access-limit-rule

Use this command to limit the number of HTTP requests per second from any IP address to your web server. The FortiWeb appliance tracks the number of requests. If the count of HTTP GET or POST requests exceeds the request limit, FortiWeb performs the action you specified.

To apply this rule, include it in an application-layer DoS-prevention policy (see [“waf application-layer-dos-prevention” on page 265](#)) and include that policy in an inline protection profile.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf layer4-access-limit-rule
  edit <rule_name>
    set access-limit-standalone-ip <limit_int>
    set access-limit-share-ip <limit_int>
    set action {alert | alert_deny | block-period}
    set real-browser-enforcement {enable | disable}
    set block-period <seconds_int>
    set severity {High | Medium | Low}
    set trigger-policy <trigger-policy_name>
    set validation-timeout <timeout_int>

  next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
access-limit-standalone-ip <limit_int>	Type the maximum number of HTTP requests allowed per second from any source IP address representing a single client. The valid range is from 0 to 65,536.	0
access-limit-share-ip <limit_int>	Type the maximum number of HTTP requests allowed per second from any source IP address shared by multiple clients behind a network address translation (NAT) device, such as a firewall or router. The valid range is from 0 to 65,536.	0

Variable	Description	Default
action {alert alert_deny block-period}	<p>Select one of the following actions that the FortiWeb appliance will perform when the count exceeds either threshold limit:</p> <ul style="list-style-type: none"> alert — Accept the request and generate an alert email and/or log message. alert_deny — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. block-period — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	alert
real-browser-enforcement {enable disable}	<p>Enable to return a JavaScript to the client to test whether it is a web browser or automated tool when it exceeds the rate limit.</p> <p>If the client either fails the test or does not return results before the timeout specified by <code>validation-timeout</code>, FortiWeb applies the specified action. If the client appears to be a web browser, FortiWeb allows the client to exceed the rate limit.</p> <p>Disable this option to apply the rate limit regardless of whether the client is a web browser (for example, Firefox) or an automated tool (for example, wget).</p>	disable
block-period <seconds_int>	Type the number of seconds to block access to the client. This applies only when the action setting is block-period. The valid range is from 0 to 10,000.	0
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium

Variable	Description	Default
trigger-policy <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
validation-timeout <timeout_int>	Specifies the maximum amount of time that FortiWeb waits for results from the client for Real Browser Enforcement.	

Example

This examples includes two rules. One blocks connections for two minutes while the other creates an alert and denies the connection.

```
config waf layer4-access-limit-rule
  edit "Web Portal HTTP Request Limit"
    set access-limit-share-ip 10
    set access-limit-standalone-ip 10
    set action block-period
    set block-period 120
    set severity Medium
    set trigger-policy "Web_Protection_Trigger"
  next
  edit "Online Store HTTP Request Limit"
    set access-limit-share-ip 5
    set access-limit-standalone-ip 5
    set action alert_deny
    set severity High
    set trigger-policy "Web_Protection_Trigger"
  next
end
```

Related topics

- [config log trigger-policy](#)
- [config waf application-layer-dos-prevention](#)
- [config waf layer4-connection-flood-check-rule](#)

waf layer4-connection-flood-check-rule

Use this command to limit the number of fully-formed TCP connections per source IP address. This effectively prevents TCP flood-style denial-of-service (DoS) attacks.

TCP flood attacks exploit the fact that servers must consume memory to maintain the state of the open connection until either the timeout, or the client or server closes the connection. This consumes some memory even if the client is not currently sending any HTTP requests.

Normally, a legitimate client will form a single TCP connection, through which they may make several HTTP requests. As a result, each client consumes a negligible amount of memory to track the state of the TCP connection. However, an attacker will open many connections with perhaps zero or one request each, until the server is exhausted and has no memory left to track the TCP states of new connections with legitimate clients.

This feature is similar to [config waf http-connection-flood-check-rule](#). However, this feature counts TCP connections per IP, while the other command counts TCP connections per session cookie.

It is also similar to [config system dos-prevention](#). However, this feature counts fully-formed TCP connections, while the anti-SYN flood feature counts partially-formed TCP connections.

To apply this rule, include it in an application-layer DoS-prevention policy (see [“waf application-layer-dos-prevention” on page 265](#)) and include that policy in an inline protection profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf layer4-connection-flood-check-rule
edit <rule_name>
    set layer4-connection-threshold <limit_int>
    set action {alert | alert_deny | block-period}
    set block-period <seconds_int>
    set severity {High | Medium | Low}
    set trigger-policy <trigger-policy_name>
next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
layer4-connection-threshold <limit_int>	Type enter the maximum number of TCP connections allowed from the same IP address. The valid range is from 0 to 65,536.	0

Variable	Description	Default
action {alert alert_deny block-period}	<p>Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the rate limit:</p> <ul style="list-style-type: none"> • <code>alert</code> — Accept the connection and generate an alert email and/or log message. • <code>alert_deny</code> — Block the connection and generate an alert email and/or log message. • <code>block-period</code> — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	alert
block-period <seconds_int>	<p>Type the length of time for which the FortiWeb appliance will block additional requests after a source IP address exceeds the rate threshold.</p> <p>The block period is shared by all clients whose traffic originates from the source IP address. The valid range is from 1 to 3,600 seconds (1 hour).</p>	1
severity {High Medium Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
trigger-policy <trigger-policy_name>	<p>Type the name of the trigger to apply when this rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre>	No default.

Example

This example illustrates a basic TCP flood check rule.

```
config waf layer4-connection-flood-check-rule
  edit "Web Portal Network Connect Limit"
    set action alert_deny
    set layer4-connection-threshold 10
    set severity Medium
```

```
        set trigger-policy "Server_Policy_Trigger"  
    next  
end
```

Related topics

- [config log trigger-policy](#)
- [config waf application-layer-dos-prevention](#)
- [config waf layer4-access-limit-rule](#)

waf padding-oracle

Use this command to create a policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS.

To apply this policy, include it in an inline web or offline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#) or [“config waf web-protection-profile offline-protection” on page 406](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf padding-oracle
  edit <padding-oracle_rule_name>
    set action {alert | alert_deny | block-period}
    set block-period <block-period_int>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    config protected-url-list
      edit <entry_index>
        set host-status {enable | disable}
        set host <host_str>
        set url-type {plain | regular}
        set protected-url <protected-url_str>
        set target {cookie parameter url}
      end
    end
```

```

next
end

```

Variable	Description	Default
<padding-oracle_rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
{alert alert_deny block-period}	Specify the action that FortiWeb takes when a request violates the rule: alert — Accept the request and generate an alert email and/or log message. alert_deny — Block the request (reset the connection) and generate an alert and/or log message. block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, define an X-header that indicates the original client's IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. Attack log messages contain Padding Oracle Attack when this feature detects a possible attack. Because this attack involves some repeated brute force, the attack log may not appear immediately, but should occur within 2 minutes, depending on your configured DoS alert interval. Caution: This setting is ignored if the value of monitor-mode is enabled. See Note: Logging and/or alert email occur only when the these features are enabled and configured. See “Logging” and “Alert email”. See Note: To use this rule set with auto-learning, select alert. If action is alert_deny or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the session information for auto-learning will be incomplete.	alert
<block-period_int>	Type the number of seconds that FortiWeb blocks subsequent requests from the client after it detects that the client has violated the rule. This setting is available only if action is block-period. The valid range is from 1 to 4,294,967,295.	1
{High Medium Low}	When rule violations are recorded in the attack log, each log message contains a Severity Level (severity_level) field. Specify the severity level FortiWeb uses when it logs a violation of this rule.	Medium

Variable	Description	Default
<trigger-policy_name>	Type the name of the trigger policy, if any, that the FortiWeb appliance uses when it logs and/or sends an alert email about a violation of the rule. See “config log trigger-policy” on page 99 . To display the list of existing triggers, type: set trigger ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
host-status {enable disable}	Specify enable to apply this rule only to HTTP requests for specific web hosts. Also specify host. Specify disable to match the rule based on the other criteria, such as the URL, but regardless of the Host: field.	disable
<host_str>	Specify which protected host names entry (either a web host name or IP address) that the Host: field of the HTTP request must be in to match the rule. This option is available only if the value of host-status is enabled. Maximum length is 255 characters.	No default.
{plain regular}	Specify how the value of protected-url is specified: plain — A literal URL. regular — A regular expression designed to match multiple URLs.	plain

Variable	Description	Default
<protected-url_str>	<p>If the value of <code>url-type</code> is <code>plain</code>, specify the literal URL that HTTP requests that match the rule contain.</p> <p>For example:</p> <pre>/profile.jsp</pre> <p>The URL must begin with a backslash (/).</p> <p>If the value of <code>url-type</code> is <code>regular</code>, specify a regular expression matching all and only the URLs to which the rule should apply.</p> <p>For example:</p> <pre>^/*\.jsp\?uid\=(.*)</pre> <p>The pattern does not require a slash (/); however, it must at least match URLs that begin with a slash, such as <code>/profile.cfm</code>.</p> <p>Do not include the domain name, such as <code>www.example.com</code>, which is specified by <code>host</code>.</p> <p>Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the FortiWeb Administration Guide.</p>	No default.
{cookie parameter url}	<p>Specify which parts of the client's requests FortiWeb examines for padding attack attempts:</p> <p><code>url</code> — A URL (for example, the parameter <code>/user/0000012FE03BC2</code> is embedded in the URL).</p> <p><code>parameter</code> — A parameter (for example, the parameter <code>/index.php?user=0000012FE03BC2</code> appended to a traditional GET or POST body).</p> <p><code>cookie</code> — A cookie.</p>	parameter

Example

This example illustrates a padding oracle rule that blocks requests to the host `www.example.com` when a parameter appended in a traditional GET URL parameter or POST body matches the specified regular expression. When a request matches the expression, FortiWeb logs or sends a high-severity message as specified in the `notification-servers1` trigger policy.

```
config waf padding-oracle
edit padding-oracle1
set action block-period
set block-period 3600
set severity High
set trigger notification-servers1
```

```
config protected-url-list
  edit 1
    set host-status enable
    set host www.example.com
    set url-type regular
    set protected-url \/profile\.jsp\?uid\=(.*)
    set target parameter
  end
```

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)

waf page-access-rule

Use this command to configure page access rules.

Page access rules define URLs that can be accessed only in a **specific order**, such as to enforce the business logic of a web application. Requests for other, non-ordered URLs may interleave ordered URLs during the client's session. Page access rules may be specific to a web host.

For example, an e-commerce application might be designed to work properly in this order:

1. A client begins a session by adding an item to a shopping cart. (/addToCart.do?*)
2. The client either views and adds additional items to the shopping cart, or proceeds directly to the checkout.
3. The client confirms the items that he or she wants to purchase. (/checkout.do)
4. The client provides shipping information. (/shipment.do)
5. The client pays for the items and shipment, completing the transaction. (/payment.do)

Sessions that begin at the shipping or payment stage should therefore be invalid. If the web application does not enforce this rule itself, it could be open to cross-site request forgery (CSRF) attacks on the payment feature. To prevent such abuse, the FortiWeb appliance could enforce the rule itself using a page access rule set with the following order:

1. /addToCart.do?item=*
2. /checkout.do?login=*
3. /shipment.do
4. /payment.do

Attempts to request /payment.do before those other URLs during a session would be denied, and generate an alert and attack log message (see [“config log disk” on page 70](#)).

To apply page access rules, select them within an inline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#).

Before you configure a page access rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see [“config server-policy allow-hosts” on page 105](#).

You can use SNMP traps to notify you when a page access rule is enforced. For details, see [“config system snmp community” on page 234](#).

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see [“Permissions” on page 47](#).



In order for page access rules to be enforced, you must also enable [http-session-management {enable | disable}](#) in the inline protection profile.

Syntax

```
config waf page-access-rule
```

```

edit <page-access-rule_name>
  config page-access-list
    edit <entry_index>
      set host <protected-hosts_name>
      set host-status {enable | disable}
      set request-file <url_str>
      set request-type {plain | regular}
    next
  end
next
end

```

Variable	Description	Default
<page-access-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999. Page access rules should be added to the set in the order which clients will be permitted to access them. For example, if a client must access /login.asp before /account.asp, add the rule for /login.asp first.	No default.
host <protected-hosts_name>	Type the name of a protected host that the Host : field of an HTTP request must be in order to match the page access rule. The maximum length is 255 characters. This setting applies only if host-status is enable.	No default.
host-status {enable disable}	Enable to apply this page access rule only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name>. Disable to match the page access rule based upon the other criteria, such as the URL, but regardless of the Host : field.	disable
request-file <url_str>	Depending on your selection in request-type {plain regular}, type either: <ul style="list-style-type: none"> the literal URL, such as /cart.php, that the HTTP request must contain in order to match the page access rule. The URL must begin with a slash (/). a regular expression, such as ^/*.php, matching all and only the URLs to which the page access rule should apply. The pattern is not required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /cart.cfm. Do not include the name of the web host, such as www.example.com, which is configured separately in host <protected-hosts_name>. The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i> .	No default.
request-type {plain regular}	Select whether request-file <url_str> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain

Example

This example allows any request to `www.example.com`, as long as it follows the expected sequence within a session for the four key shopping cart URLs (`/addToCart.do`, `/checkout.do`, `/shipment.do`, then `/payment.do`).

```
config waf page-access-rule
  edit "page-access-rule1"
    config page-access-list
      edit 1
        set host "www.example.com"
        set host-status enable
        set request-file "/addToCart.do?item=*"
        set request-type regular
      next
      edit 2
        set host "www.example.com"
        set host-status enable
        set request-file "/checkout.do?login=*"
        set request-type regular
      next
      edit 3
        set host "www.example.com"
        set host-status enable
        set request-file "/shipment.do"
        set request-type plain
      next
      edit 4
        set host "www.example.com"
        set host-status enable
        set request-file "/payment.do"
        set request-type plain
      next
    end
  next
end
```

Related topics

- [config server-policy allow-hosts](#)
- [config system snmp community](#)
- [config waf web-protection-profile inline-protection](#)

waf parameter-validation-rule

Use this command to configure parameter validation rules, each of which is a group of input rule entries.

To apply parameter validation rules, select them within an inline or offline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#) or [“config waf web-protection-profile offline-protection” on page 406](#).

Before you can configure parameter validation rules, you must first configure one or more input rules. For details, see [“config waf input-rule” on page 327](#).

You can use SNMP traps to notify you when a parameter validation rule is enforced. For details, see [“config system snmp community” on page 234](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf parameter-validation-rule
  edit <rule_name>
    config input-rule-list
      edit <entry_index>
        set input-rule <input-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
input-rule <input-rule_name>	Type the name of an input rule to use in the parameter validation rule. The maximum length is 35 characters. To display the list of existing input rules, type: <code>set input-rule ?</code>	No default.

Example

This example configures a parameter validation rule that applies two input rules.

```
config waf parameter-validation-rule
  edit "parameter_validator1"
    config input-rule-list
      edit 1
        set input-rule "input_rule1"
```

```
        next
        edit 2
            set input-rule "input_rule2"
        next
    end
next
end
```

Related topics

- [config waf input-rule](#)
- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)

waf signature

Use this command to configure server protection rules.

There are several security features specifically designed to protect web servers from known attacks. You can configure defenses against:

- cross-site scripting (XSS)
- SQL injection and many other code injection styles
- generic attacks
- known exploits
- trojans/viruses
- information disclosure
- bad robots
- credit card data leaks

FortiWeb scans:

- HTTP headers
- parameters in the URL of HTTP GET requests
- parameters in the body of HTTP POST requests
- XML in the body of HTTP POST requests (if `xml-protocol-detection {enable | disable}` is enabled)
- cookies

In addition to scanning standard requests, signatures can also scan action message format 3.0 (AMF3) binary inputs used by Adobe Flash clients to communicate with server-side software and XML. For more information, see `amf3-protocol-detection {enable | disable}` and `malformed-xml-check {enable | disable}` (for inline protection profiles) or `amf3-protocol-detection {enable | disable}` (for offline protection profiles).

Known attack signatures can be updated. For information on uploading a new set of attack definitions, see the *FortiWeb Administration Guide*. You can also create your own. See “[config waf custom-protection-rule](#)” on page 282.

Each server protection rule can be configured with the severity and notification settings (“trigger”) that, in combination with the action, determines how each violation will be handled.

For example, attacks categorized as cross-site scripting and SQL injection could have the action set to `alert_deny`, the severity set to `High`, and a trigger set to deliver an alert email each time these rule violations are detected. Specific signatures in those categories, however, might be disabled, set to `log/alert` instead, or exempt requests to specific host names/URLs.

To override category-wide actions for a specific signature, configure:

- `config signature_disable_list` — Disable a specific signature ID (e.g. 040000007), even if the category in general (e.g. *SQL Injection (Extended)*) is enabled.
- `config sub_class_disable_list` — Disable a subcategory of signatures (e.g. *Session Fixation*), even if the category in general (e.g. *General Attacks*) is enabled.
- `config alert_only_list` — Only log/alert when detecting the attack, even if the category in general is configured to block.
- `config filter_list` — Exempt specific host name and/or URL combinations from scanning with this signature.

Before configuring a server protection rule, if you want to configure your own attack or data leak signatures, you must also configure custom server protection rules. For details, see [“config waf custom-protection-group” on page 280](#).

To apply server protection rules, select them within an inline or offline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#) or [“config waf web-protection-profile offline-protection” on page 406](#).

You can use SNMP traps to notify you when an attack or data leak has been detected. For details, see [“config system snmp community” on page 234](#).



Alternatively, you can automatically configure a server protection rule that detects all attack types by generating a default auto-learning profile. For details, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf signature
edit <signature-set_name>
  set credit-card-detection-threshold <instances_int>
  [set custom-protection-group <group_name>]
  config main_class_list
    edit {010000000 | 020000000 | 030000000 | 040000000 |
050000000 | 060000000 | 070000000 | 080000000 | 090000000 |
100000000}
      set action {alert | alert_deny | block-period | only_erase |
alert_erase | redirect | send_403_forbidden}
      set block-period <seconds_int>
      set severity {Low | Medium | High}
      set trigger <trigger-policy_name>
    next
  end
  config signature_disable_list
    edit <signature-id_str>
    next
  end
  config sub_class_disable_list
    edit {010000000 | 020000000 | 030000000 | 040000000 |
050000000 | 060000000 | 070000000 | 080000000 | 090000000 |
100000000}
    next
  end
  config alert_only_list
    edit <signature-id_str>
    next
  end
```

```

config filter_list
  edit <entry_index>
    set signature_id <signature-id_str>
    set host-status {enable | disable}
    set host <protected-hosts_name>
    set type {plain | regular}
    set request-file <url_str>
  next
end
next
end

```

Variable	Description	Default
<signature-set_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
credit-card-detection-threshold <instances_int>	Type 0 to report any credit card number disclosures, or type a threshold if the web page must contain a number of credit cards that equals or exceeds the threshold in order to trigger the credit card number detection feature. For example, to ignore web pages with only one credit card number, but to detect when a web page containing two or more credit cards, enter 2. The valid range is from 0 to 128 instances.	0
custom-protection-group <group_name>	Type the name of the custom signature group to be used, if any. The maximum length is 35 characters. To display the list of existing custom signature groups, type: set custom-protection-group ?	No default.
{010000000 020000000 030000000 040000000 050000000 060000000 070000000 080000000 090000000 100000000}	Type the ID of a signature class (or, for subclass overrides, the subclass ID). To display the list of signature classes, type: edit ?	No default.

Variable	Description	Default
<pre> action {alert alert_deny block-period only_erase alert_erase redirect send_403_forbidden} </pre>	<p>Select which action the FortiWeb appliance will take when it detects a signature match.</p> <p>Note: This is not a single setting. Available actions may vary slightly, depending on what is possible for each specific type of attack/information disclosure.</p> <ul style="list-style-type: none"> • alert — Accept the request and generate an alert email and/or log message. Note: Does <i>not</i> cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) • alert_deny — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. • block-period — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you <i>must</i> also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block <i>all</i> connections when it detects a violation of this type. • only_erase — Hide sensitive information in replies from the web server (sometimes called “cloaking”). Block the request or remove the sensitive information, but do not generate an alert email and/or log message. Caution: This option is not supported in offline protection mode. • alert_erase — Hide replies with sensitive information (sometimes called “cloaking”). Block the reply (or reset the connection) or remove the sensitive information, and generate an alert email and/or log message. Note: This option is not fully supported in offline protection mode. Effects will be identical to <code>alert</code>; sensitive information will not be blocked or erased. 	<p>alert</p>

Variable	Description	Default
	<ul style="list-style-type: none"> <code>redirect</code> — Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <code>redirect-url <redirect_fqdn></code> and <code>rdt-reason {enable disable}</code>. <code>send_403_forbidden</code> — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	
<code>block-period</code> <code><seconds_int></code>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>The valid range is from 1 to 3,600. The setting is applicable only if <code>action</code> is <code>period-block</code>.</p> <p>Note: This is not a single setting. You can configure the block period separately for each signature category.</p>	60
<code>severity {Low Medium High}</code>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> Low Medium High <p>Note: This is not a single setting. You can configure the severity separately for each signature category.</p>	Medium
<code>trigger <trigger-policy_name></code>	<p>Type the name of the trigger, if any, to apply when a protection rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing triggers, type:</p> <pre>set trigger ?</pre> <p>Note: This is not a single setting. You can configure a different trigger for each signature category.</p>	No default.
<code><signature-id_str></code>	<p>Type the ID of a specific signature that you want to disable.</p> <p>Some signatures often cause false positives and are disabled by default. To display a list, type:</p> <pre>edit ?</pre>	No default.

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 32.	No default.
signature_id <signature-id_str>	Type the ID of a specific signature that you want to disable when the request matches a specific Host : name and/or URL. Also configure <code>host-status {enable disable}</code> , <code>host-status {enable disable}</code> , and <code>request-file <url_str></code> .	No default.
host <protected-hosts_name>	Type the name of a protected host that the Host : field of an HTTP request must be in order to match the start page rule. The maximum length is 255 characters. This setting applies only if <code>host-status</code> is <code>enable</code> .	No default.
host-status {enable disable}	Enable to apply this start page rule only to HTTP requests for specific web hosts. Also configure <code>host <protected-hosts_name></code> . Disable to match the start page rule based upon the other criteria, such as the URL, but regardless of the Host : field.	disable
type {plain regular}	Select whether <code>request-file <url_str></code> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
request-file <url_str>	Depending on your selection in <code>type {plain regular}</code> , type either: <ul style="list-style-type: none"> the literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the signature exception. The URL must begin with a slash (/). a regular expression, such as <code>^/* .php</code>, matching all and only the URLs to which the signature exception should apply. The pattern is not required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the name of the web host, such as <code>www.example.com</code> , which is configured separately in <code>host <protected-hosts_name></code> . The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the FortiWeb Administration Guide .	No default.

Example

This example enables both the Trojans (070000000) and XSS (010000000) classes of signatures, setting them to result in attack logs with a `severity_level` field of High, and using the email and SNMP settings defined in `notification-servers1`. It also enables use of custom attack and data leak signatures in the set named `custom-signature-group1`.

This example disables by ID a signature that is known to cause false positives (080200001). It also makes an exception (`config filter_list`) by ID for a specific signature (070000001) for a URL (`/virus-sample-upload`) on a host (`www.example.com`) that is used by security researchers to receive virus samples.

```
config waf signature
edit "attack-signatures1"
set custom-protection-group "custom-signature-group1"
```



```

config main_class_list
  edit "010000000"
    set severity High
    set trigger "notification-servers1"
  next
  edit "070000000"
    set severity High
    set trigger "notification-servers1"
  next
end
config signature_disable_list
  edit "080200001"
  next
end
config filter_list
  edit 1
    set signature_id "070000001"
    set host-status enable
    set host "www.example.com"
    set request-file "/virus-sample-upload"
  next
end
next
end

```

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config system snmp community](#)
- [config waf custom-protection-group](#)
- [config log trigger-policy](#)

waf site-publish-helper policy

Use this command to group together web applications that you want to publish.

Before you configure site publishing policies, you must first define the individual sites that will be a part of the group. For details, see [“config waf site-publish-helper rule” on page 363](#).

To apply this policy, include it in an inline web protection profile. See [“config waf web-protection-profile inline-protection” on page 390](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf site-publish-helper policy
  edit <site-publish-policy_name>
    config rule
      edit <entry_index>
        set rule-name <site-publish-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
<site-publish-policy_name>	Type the name of a new or existing policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
rule-name <site-publish-rule_name>	Type the name of an existing rule.	No default.

Example

For an example, see [“waf site-publish-helper rule” on page 363](#).

Related topics

- [config waf site-publish-helper rule](#)
- [config waf web-protection-profile inline-protection](#)

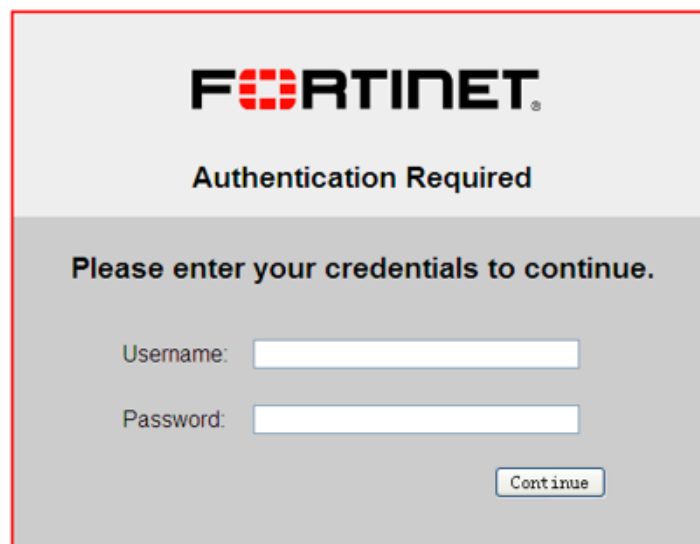
waf site-publish-helper rule

Use this command to configure access control, authentication, and, optionally, SSO for your web applications.

If:

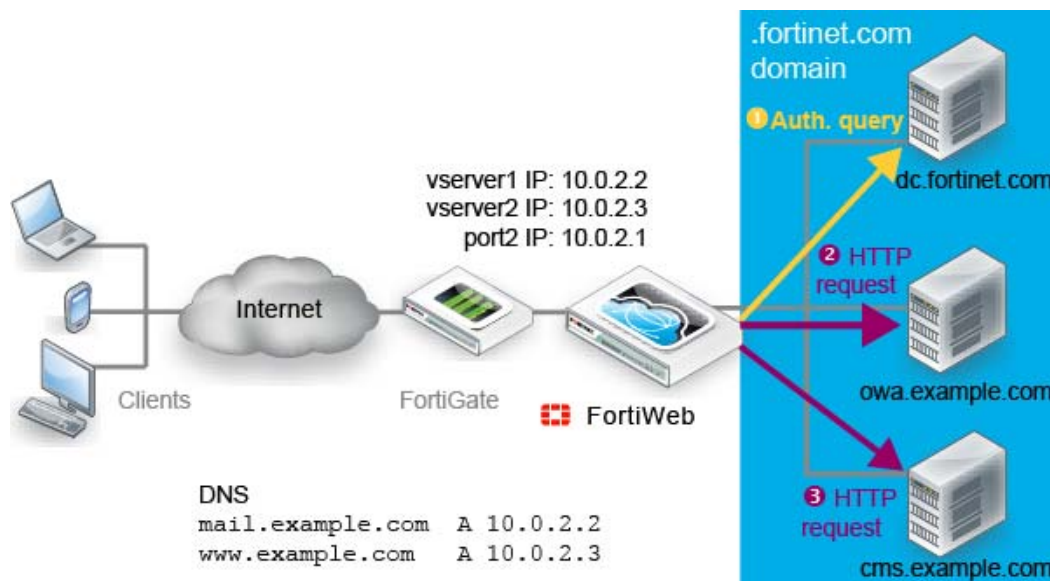
- your users will be accessing multiple web applications on your domain, and
- you have defined accounts centrally on an LDAP (such as Microsoft Active Directory) or RADIUS server

you may want to configure single sign-on (SSO) and combination access control and authentication (called “site publishing” in the GUI) instead of configuring simple HTTP authentication rules. SSO provides a benefit over HTTP authentication rules: your users will not need to authenticate each time they access separate web applications in your domain. When FortiWeb receives the first request, it will return (depending on your configuration) an HTML authentication form or HTTP `WWW-Authenticate`: code to the client.

A screenshot of a Fortinet authentication form. At the top, the Fortinet logo is displayed in black and red. Below the logo, the text "Authentication Required" is centered. Underneath, the instruction "Please enter your credentials to continue." is shown. There are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. A "Continue" button is located at the bottom right of the form.

FortiWeb sends the client’s credentials in a query to the authentication server. Once the client is successfully authenticated, if the web application supports HTTP authentication and you have configured delegation, FortiWeb forwards the credentials to the web application. The server’s response is returned to the client. Until the session expires, subsequent requests from the client

to the same or other web applications in the same domain do not require the client to authenticate..



For example, you may prefer SSO if you are using FortiWeb to replace your discontinued Microsoft Threat Management Gateway, using it as a portal for multiple applications such as SharePoint, Outlook Web Application, and/or IIS. Your users will only need to authenticate once while using those resources.

Before you configure site publishing, you must first define the queries to your authentication server. For details, see [“config user ldap-user” on page 245](#) or [“config user radius-user” on page 252](#).

To use this command, your administrator account’s access control profile must have either w or rw permission to the wafgrp area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf site-publish-helper rule
edit <site-publish-rule_name>
set status {enable | disable}
set req-type {plain | regular}
set published-site <host_fqdn>
set path <url_str>
set client-auth-method {html-form-auth | http-auth}
[set Published-Server-Logoff-Path <url_str>]
set auth-method {ldap | radius}
set ldap-server <query_name>
set radius-server <query_name>
set alert-type {all | fail | none | success}
set auth-delegation {http-basic | no-delegation}
set sso-support {enable | disable}
set sso-domain <domain_str>
```

```

next
end

```

Variable	Description	Default
<site-publish-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
status {enable disable}	Enable to activate this rule. This can be used to temporarily deactivate access to a single web application without removing it from a site publishing policy.	enable
alert-type {all fail none success}	Select which site publishing-related authentication events the FortiWeb appliance will log and/or send an alert email about. <ul style="list-style-type: none"> all fail success none <p>Event log messages contain the user name, authentication type, success or failure, and source address (for example, User jdoe [Site Publish] login successful from 172.0.2.5) when an end-user successfully authenticates. A similar message is recorded if the authentication fails (for example, User hackers [Site Publish] login failed from 172.0.2.5).</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p>	none
auth-delegation {http-basic no-delegation}	Select what FortiWeb should do after the client successfully authenticates with the authentication server, either: <ul style="list-style-type: none"> http-basic — Use HTTP Authorization: headers with Base64 encoding to forward the client’s credentials to the web application. Typically you should select this option if the web application supports HTTP protocol-based authentication. no-delegation — Do not send the client’s credentials to the web application. Typically you should select this option if the web application uses HTML form-based authentication, or has no authentication. <p>Note: If the web application uses form-based authentication, the client will be required to authenticate twice: once with FortiWeb, and then once again with the web application’s HTML form.</p>	no-delegation
auth-method {ldap radius}	Depending on which query you want to use to authenticate clients, select either LDAP or RADIUS.	ldap

Variable	Description	Default
<code>client-auth-method {html-form-auth http-auth}</code>	<p>Select which method FortiWeb should use to present the authentication dialog to the requesting client, either:</p> <ul style="list-style-type: none"> return an HTML web page with an authentication form (<code>html-form-auth</code>), or return an HTTP AUTH code so that the browser displays its own dialog (<code>http-auth</code>) 	<code>html-form-auth</code>
<code>ldap-server <query_name></code>	Type the name of the authentication query that FortiWeb will use to pass credentials to your authentication server.	No default.
<code>path <url_str></code>	Type the URL of the request for the web application, such as <code>/owa</code> . It must begin with a forward slash (<code>/</code>).	No default.
<code>Published-Server-Logoff-Path <url_str></code>	<p>Optionally, type the URL of the request that a client sends to log out of the application, such as:</p> <p><code>/owa/auth/logoff.aspx?Cmd=logoff</code></p> <p>When logging out of the web application, the client will be redirected to FortiWeb's authentication dialog.</p> <p>This setting appears only if <code>client-auth-method {html-form-auth http-auth}</code> is <code>html-form-auth</code>.</p>	No default.
<code>published-site <host_fqdn></code>	<p>Depending on your selection in <code>req-type {plain regular}</code>, type either:</p> <ul style="list-style-type: none"> the literal <code>Host</code>: name, such as <code>sharepoint.example.com</code>, that the HTTP request must contain in order to match the rule. a regular expression, such as <code>^*\.example\.edu</code>, matching all and only the host names to which the rule should apply. <p>The maximum length is 255 characters.</p> <p>Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i>.</p>	No default.
<code>radius-server <query_name></code>	Type the name of the authentication query that FortiWeb will use to pass credentials to your authentication server.	No default.
<code>req-type {plain regular}</code>	Select whether <code>published-site <host_fqdn></code> will contain a literal FQDN (<code>plain</code>), or a regular expression designed to match multiple host names or fully qualified domain names (<code>regular</code>).	<code>plain</code>
<code>sso-domain <domain_str></code>	Type the domain suffix of <code>Host</code> : names that will be allowed to share this rule's authentication sessions, such as <code>.example.com</code> . Include the period (<code>.</code>) that precedes the host's name.	No default.
<code>sso-support {enable disable}</code>	<p>Enable for single sign-on support.</p> <p>For example, if this web site is <code>www1.example.com</code> and the SSO domain is <code>.example.com</code>, once a client has authenticated with that site, it can access <code>www2.example.com</code> without authenticating a second time.</p> <p>Site publishing SSO sessions exist on FortiWeb only; they are not synchronized to the authentication and/or accounting server, and therefore SSO is not shared with non-web applications. For SSO with other protocols, consult the documentation for your FortiGate or other firewall.</p>	<code>disable</code>

Example

This example configures a site publisher with SSO for both Outlook and Sharepoint on the example.com domain.

```
config waf site-publish-helper rule
  edit "Outlook"
    set published-site ^*\..example\..edu
    set ldap-server "LDAP query 1"
    set auth-delegation http-basic
    set sso-support enable
    set sso-domain .example.edu
    set path /owa
    set alert-type fail
    set Published-Server-Logoff-Path /owa/auth/logoff.aspx?Cmd=logoff
  next
  edit "Sharepoint"
    set published-site ^*\\.example\\.edu
    set req-type regular
    set radius-server "RADIUS query 1"
    set auth-delegation http-basic
    set sso-support enable
    set sso-domain .example.edu
    set path /sharepoint
    set alert-type fail
  next
end
config waf site-publish-helper policy
  edit "example_com_apps"
    config rule
      edit 1
        set rule-name Outlook
      next
      edit 2
        set rule-name Sharepoint
      next
    end
  next
end
```

Related topics

- [config waf site-publish-helper policy](#)
- [config log trigger-policy](#)
- [config server-policy allow-hosts](#)
- [config waf web-protection-profile inline-protection](#)

waf start-pages

Use this command to configure start page rules.

When a start page group is selected in the inline protection profile, HTTP clients must begin from a valid start page in order to initiate a valid session.

For example, you may wish to specify that HTTP clients of an e-commerce web site must begin their session from either an item view or the first stage of the shopping cart checkout, and cannot begin a valid session from the third stage of the shopping cart checkout.

To apply start pages, select them within an inline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#).

Before you configure a start page rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see [“config server-policy allow-hosts” on page 105](#).

You can use SNMP traps to notify you when a start page rule is enforced. For details, see [“config system snmp community” on page 234](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf start-pages
  edit <start-page-rule_name>
    set action {alert | alert_deny | block-period | redirect |
send_403_forbidden}
    set block-period <seconds_int>
    set severity {Low | Medium | High}
    set trigger <trigger-policy_name>
    config start-page-list
      edit <entry_index>
        set host <protected-hosts_name>
        set host-status {enable | disable}
        set request-file <url_str>
        set request-type {plain | regular}
        set default {yes | no}
      next
    end
```



```

next
end

```

Variable	Description	Default
<start-page-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
action {alert alert_deny block-period redirect send_403_forbidden}	Select one of the following actions that the FortiWeb appliance will perform when an HTTP request that initiates a session does not begin with one of the allowed start pages. <ul style="list-style-type: none"> • <code>alert</code> — Accept the request and generate an alert email and/or log message. • <code>alert_deny</code> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. • <code>block-period</code> — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. • <code>redirect</code> — Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <code>redirect-url <redirect_fqdn></code> and <code>rdt-reason {enable disable}</code>. • <code>send_403_forbidden</code> — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	No default.
block-period <seconds_int>	If <code>action</code> is <code>block-period</code> , type, specify the number of seconds that the connection will be blocked. The valid range is from 1 to 3,600 seconds.	1
severity {Low Medium High}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low

Variable	Description	Default
trigger <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host <protected-hosts_name>	Type the name of a protected host that the Host: field of an HTTP request must be in order to match the start page rule. The maximum length is 255 characters. This setting applies only if host-status is enable.	No default.
host-status {enable disable}	Enable to apply this start page rule only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name> . Disable to match the start page rule based upon the other criteria, such as the URL, but regardless of the Host: field.	disable
request-file <url_str>	Depending on your selection in request-type {plain regular} , type either: <ul style="list-style-type: none"> the literal URL, such as /index.php, that the HTTP request must contain in order to match the start page rule. The URL must begin with a slash (/). a regular expression, such as ^/*\.php, matching all and only the URLs to which the start page rule should apply. The pattern is not required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. Do not include the name of the web host, such as www.example.com, which is configured separately in host <protected-hosts_name> . The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the FortiWeb Administration Guide .	No default.
request-type {plain regular}	Select whether request-file <url_str> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
default {yes no}	Type yes to use the page as the default for HTTP requests that either: <ul style="list-style-type: none"> do not specify a URL do not specify the URL of a valid start page (only if you have selected redirect from action) Otherwise, type no.	no

Example

This example redirects clients to the default start page, /index.html, if clients request a page that is not one of the valid start pages (/index.html or /cart/login.jsp). Redirection will

occur only if the request is destined for one of the virtual or real hosts defined in the protected hosts group named `example_com_hosts`.

```
config waf start-pages
  edit "start-page-rule1"
    edit 1
      set host "example_com"
      set host-status enable
      set request-file "/index.html"
      set default yes
    next
  edit 2
    set host "example_com_hosts"
    set host-status enable
    set request-file "/cart/login.jsp"
    set default no
  next
next
end
```

Related topics

- [config log trigger-policy](#)
- [config server-policy allow-hosts](#)
- [config waf web-protection-profile inline-protection](#)
- [config system snmp community](#)

waf url-access url-access-policy

Use this command to configure a set of URL access rules that define HTTP requests that will be allowed or denied.

Before using this command, you must first define your URL access rules (see [“waf url-access url-access-rule” on page 374](#)).

To apply URL access policies, select them within an inline or offline protection profile. For details see, [“config waf web-protection-profile inline-protection” on page 390](#) or [“config waf web-protection-profile offline-protection” on page 406](#).

You can use SNMP traps to notify you when a URL access rule is enforced. For details, see [“config system snmp community” on page 234](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf url-access url-access-policy
  edit <url-access-policy_name>
    config rule
      edit <entry_index>
        set url-access-rule-name <url-access-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
<url-access-policy_name>	Type the name of the new or existing URL access policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
url-access-rule-name <url-access-rule_name>	Type the name of the existing URL access rule to add to the policy. The maximum length is 35 characters.	No default.

Example

This example adds two rules to the policy, with the first one set to priority level 0, and the second one set to priority level 1. The rule with priority 0 would be applied first.

```
config waf url-access url-access-policy
  edit "URL-access-set2"
```

```
config rule
  edit 1
    set url-access-rule-name "URL Access Rule 1"
  next
  edit 2
    set url-access-rule-name "Blocked URL"
  next
next
end
```

Related topics

- [config waf url-access url-access-rule](#)
- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)

waf url-access url-access-rule

Use this command to configure URL access rules that define the HTTP requests that are allowed or denied based on their host name and URL.

Typically, for example, access to administrative panels for your web application should **only** be allowed if the client's source IP address is an administrator's computer on your private management network. Unauthenticated access from unknown locations increases risk of compromise. Best practice dictates that such risk should be minimized.

To apply URL access rules, first group them within a URL access policy. For details see, [“config waf url-access url-access-policy” on page 372](#).

You can use SNMP traps to notify you when a URL access rule is enforced. For details, see [“config system snmp community” on page 234](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf url-access url-access-rule
edit <url-access-rule_name>
    set action {alert_deny | continue | pass}
    set host <protected-hosts_name>
    set host-status {enable | disable}
    set severity {Low | Medium | High}
    set trigger <trigger-policy_name>
    config match-condition
        edit <entry_index>
            set type {regular-expression | simple-string}
            set reverse-match {yes | no}
            set reg-exp <object_pattern>
            set sip-address-check {enable | disable}
            set sip-address-type {sdomain | sip}
            set sip-address-domain <fqdn_str>
            set sip-address-value <client_ip>
        next
    next
```

```

end
next
end

```

Variable	Description	Default
<code><url-access-rule_name></code>	<p>Type the name of a new or existing rule. The maximum length is 35 characters.</p> <p>To display the list of existing rules, type:</p> <pre>edit ?</pre>	No default.
<code>action {alert_deny continue pass}</code>	<p>Select which action the FortiWeb appliance will take when a request matches the URL access rule.</p> <ul style="list-style-type: none"> <code>alert_deny</code> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. <code>continue</code> — Generate an alert and/or log message, then continue by evaluating any subsequent rules defined in the web protection profile (see “debug flow trace” on page 455). If no other rules are violated, allow the request. If multiple rules are violated, a single request will generate multiple attack log messages. <code>pass</code> — Allow the request. Do not generate an alert and/or log message. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select <code>pass</code>. If the action is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	alert
<code>host <protected-hosts_name></code>	<p>Type the name of a protected host that the <code>Host:</code> field of an HTTP request must be in order to match the rule. The maximum length is 255 characters.</p> <p>This setting is used only if <code>host-status</code> is enable.</p>	No default.
<code>host-status {enable disable}</code>	<p>Enable to require that the <code>Host:</code> field of the HTTP request match a protected hosts entry in order to match the rule. Also configure <code>host <protected-hosts_name></code>.</p>	disable
<code>severity {Low Medium High}</code>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when a blacklisted IP address attempts to connect to your web servers:</p> <ul style="list-style-type: none"> Low Medium High 	No default.

Variable	Description	Default
trigger <trigger-policy_name>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a blacklisted IP address's attempt to connect to your web servers (see “config log trigger-policy” on page 99). The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
reg-exp <object_pattern>	<p>Depending on your selection in type {regular-expression simple-string} and reverse-match {yes no}, type a regular expression that defines either all matching or all non-matching URLs. Then, also configure reverse-match {yes no}.</p> <p>For example, for the URL access rule to match all URLs that begin with /wordpress, you could enter ^/wordpress, then, in reverse-match {yes no}, select no.</p> <p>The pattern is not required to begin with a slash (/). The maximum length is 255 characters.</p> <p>Note: Regular expressions beginning with an exclamation point (!) are not supported. Instead, use reverse-match {yes no}.</p>	No default.
reverse-match {yes no}	<p>Indicate how to use reg-exp <object_pattern> when determining whether or not this rule's condition has been met.</p> <ul style="list-style-type: none"> no — If the simple string or regular expression does match the request URL, the condition is met. yes — If the simple string or regular expression does not match the request URL, the condition is met. <p>The effect is equivalent to preceding a regular expression with an exclamation point (!).</p>	no
sip-address-check {enable disable}	Enable to add the client's source IP address as a criteria for matching the URL access rule. Also configure sip-address-type {sdomain sip} and either sip-address-domain <fqdn_str> or sip-address-value <client_ip> .	disable
sip-address-domain <fqdn_str>	<p>Type the fully qualified domain name (FQDN) that a client source IP must reverse resolve (RDNS query) in order to match.</p> <p>This option appears only if sip-address-type {sdomain sip} is domain.</p>	No default.
sip-address-type {sdomain sip}	<p>Select how you want to define matching client source IPs, by either:</p> <ul style="list-style-type: none"> sip — Configure sip-address-value <client_ip>. sdomain — Configure sip-address-domain <fqdn_str>. 	sip

Variable	Description	Default
<code>sip-address-value</code> <code><client_ip></code>	Enter one of the following values: <ul style="list-style-type: none"> A single IP address that a client source IP must match, such as a trusted private network IP address (e.g. an administrator's computer, 172.16.1.20). A range or addresses (for example, 172.22.14.1-172.22.14.255 or 10:200::10:1-10:200:10:100). This option is available only if <code>sip-address-type {sdomain sip}</code> is sip.	0.0.0.0
<code>type {regular-expression simple-string}</code>	Select how to use the text in <code>reg-exp <object_pattern></code> to determine whether or not a request URL meets the conditions for this rule. <ul style="list-style-type: none"> <code>simple-string</code> — The text is a string that request URLs must match exactly. <code>regular-expression</code> — The text is a regular expression that defines a set of matching URLs. 	No default.

Example

This example defines two sets of URL access rules.

The first set, Blocked URL, defines two URL match conditions: one uses a simple string to match an administrative page, and the other uses a regular expression to match a set of dynamic URLs for statistics pages.

The second set, Allowed URL, defines a single match condition that uses a regular expression to match all dynamic forms of the index page.

Actual blocking or allowing of the URLs, however, would not occur until a policy applies these URL access rules, and sets an action that the FortiWeb appliance will perform when an HTTP request matches either rule set.

```
config waf url-access url-access-rule
  edit "Blocked URL"
    config match-condition
      edit 1
        set type simple-string
        set reg-exp "/admin.php"
      next
      edit 2
        set type regular-expression
        set reverse-match no
        set reg-exp "statistics.php*"
      next
    end
  next
  edit "Allowed URL"
```

```
config match-condition
  edit 1
    set type regular-expression
    set reverse-match no
    set reg-exp "index.php*"
  next
end
next
end
```

Related topics

- [config waf web-protection-profile inline-protection](#)
- [config waf web-protection-profile offline-protection](#)
- [config waf url-access url-access-policy](#)

waf url-rewrite url-rewrite-policy

Use this command to group URL rewrite rules.

Before you can configure a URL rewrite group, you must first configure any URL rewriting rules that you want to include. For details, see [“config waf url-rewrite url-rewrite-rule” on page 380](#).

To apply a URL rewriting group, select it in an inline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf url-rewrite url-rewrite-policy
  edit <url-rewrite-group_name>
    config rule
      edit <entry_index>
        set url-rewrite-rule-name <url-rewrite-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
<url-rewrite-group_name>	Type the name of the URL rewriting rule group. The maximum length is 35 characters. To display the list of existing group, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
url-rewrite-rule-name <url-rewrite-rule_name>	Type the name of an existing URL rewriting rule that you want to include in the group. The maximum length is 35 characters.	No default.

Related topics

- [config waf url-rewrite url-rewrite-rule](#)
- [config waf web-protection-profile inline-protection](#)

waf url-rewrite url-rewrite-rule

Use this command to configure URL rewrite rules or to redirect requests.

Rewriting or redirecting HTTP requests and responses is popular, and can be done for many reasons.

Similar to error message cloaking, URL rewriting can prevent the disclosure of underlying technology or web site structures to HTTP clients.

For example, when visiting a blog web page, its URL might be:

```
http://www.example.com/wordpress/?feed=rss2
```

Simply knowing the file name, that the blog uses PHP, its compatible database types, and the names of parameters via the URL could help an attacker to craft an appropriate attack for that platform. By rewriting the URL to something more human-readable and less platform-specific, the details can be hidden:

```
http://www.example.com/rss2
```

Aside from for security, rewriting and redirects can be for aesthetics or business reasons. Financial institutions can transparently redirect customers that accidentally request HTTP:

```
http://bank.example.com/login
```

to authenticate and do transactions on their secured HTTPS site:

```
https://bank.example.com/login
```

Additional uses could include:

- During maintenance windows, requests can be redirected to a read-only server.
- International customers can use global URLs, with no need to configure the back-end web servers to respond to additional HTTP virtual host names.
- Shorter URLs with easy-to-remember phrases and formatting are easier for customers to understand, remember, and return to.

Much more than their name implies, “URL rewriting rules” can do all of those things, and more:

- redirect HTTP requests to HTTPS
- rewrite the URL line in the header of an HTTP request
- rewrite the `Host :` field in the header of an HTTP request
- rewrite the `Referer :` field in the header of an HTTP request
- redirect requests to another web site
- send a `403 Forbidden` response to a matching HTTP requests
- rewrite the HTTP location line in the header of a matching redirect response from the web server
- rewrite the body of an HTTP response from the web server



Rewrites/redirects are not supported in all modes. See the [FortiWeb Administration Guide](#).

To use a URL rewriting rule, add it to a policy. For details, see “[config waf url-rewrite url-rewrite-policy](#)” on page 379.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf url-rewrite url-rewrite-rule
  edit <url-rewrite-rule_name>
    set action {403-forbidden | redirect | redirect-301 | http-body-rewrite | http-
      header-rewrite | location-rewrite}
    set host {<server_fqdn> | <server_ipv4> | <host_pattern>}
    set host-status {enable | disable}
    set host-use-pserver {enable | disable}
    set url <replacement-url_str>
    set url-status {enable | disable}
    set location <location_str>
    set location_replace <location_str>
    set referer-status {enable | disable}
    set referer <referer-url_str>
    set referer-use-pserver {enable | disable}
    set body_replace <replacement_str>
  config match-condition
    edit <entry_index>
      set content-filter {enable | disable}
      set content-type-set {text/html text/plain text/javascript
        application/xml(or)text/xml application/javascript
        application/soap+xml application/x-javascript}
      set HTTP-protocol {http | https}
      set is-essential {yes | no}
      set object {http-host | http-reference | http-url}
      set protocol-filter {enable | disable}
      set reg-exp <object_pattern>
      set reverse-match {yes | no}
    next
  end
```

```

next
end

```

Variable	Description	Default
<url-rewrite-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
action {403-forbidden redirect redirect-301 http-body-rewrite http-header-rewrite location-rewrite}	Select either: <ul style="list-style-type: none"> • 403-forbidden — Send a 403 (Forbidden) response to the client. • redirect — Send a 302 (Moved Temporarily) response to the client, with a new Location: field in the HTTP header. • redirect-301 — Send a 301 (Moved Permanently) response to the client, with a new Location: field in the HTTP header. • http-body-rewrite — Replace the specific HTTP content in the body of responses. • http-header-rewrite — Rewrite the host, referer and request URL fields in HTTP header. • location-rewrite — Rewrite the location string in a 302 redirect. 	http-header-rewrite

Variable	Description	Default
host {<server_fqdn> <server_ipv4> <host_pattern>}	<p>Type the FQDN of the host, such as <code>store.example.com</code>, to which the request will be redirected. The maximum length is 255 characters.</p> <p>This option is available only when <code>host-status</code> is enabled and <code>action</code> is <code>http-header-rewrite</code>.</p> <p>This field supports back references such as <code>\$0</code> to the parts of the original request that matched any capture groups that you entered in <code>reg-exp <object_pattern></code> for each object in the condition table. (A capture group is a regular expression, or part of one, surrounded in parentheses.)</p> <p>Use <code>\$n</code> ($0 \leq n \leq 9$) to invoke a substring, where <code>n</code> is the order of appearance of the regular expression, from left to right, from outside to inside, then from top to bottom.</p> <p>For example, regular expressions in the condition table in this order:</p> <pre>(a) (b) (c (d)) (e) (f)</pre> <p>would result in invokable variables with the following values:</p> <ul style="list-style-type: none"> • <code>\$0</code> — a • <code>\$1</code> — b • <code>\$2</code> — cd • <code>\$3</code> — d • <code>\$4</code> — e • <code>\$5</code> — f 	No default.
host-status {enable disable}	<p>Enable to rewrite the <code>Host:</code> field or host name part of the <code>Referer:</code> field.</p> <p>When disabled, the FortiWeb appliance preserves the value from the client's request when rewriting it.</p> <p>This option is available only when <code>action</code> is <code>http-header-rewrite</code>.</p>	disable
host-use-pserver {enable disable}	<p>Enable this when you have a server farm for server balance or content routing. In this case you do not know which server in the server farm the FortiWeb appliance will use. When FortiWeb processes the request, it sets the value for the actual host.</p> <p>This option is available only when <code>host-status</code> is enabled and <code>action</code> is <code>http-header-rewrite</code>. Any setting you make for <code>host</code> is ignored.</p>	disable

Variable	Description	Default
url <replacement-url_str>	<p>Type the string, such as /catalog/item1, that will replace the request URL. The maximum length is 255 characters.</p> <p>This option is available only when url-status is enabled and action is http-header-rewrite.</p> <p>Do not include the name of the web host, such as www.example.com, nor the protocol, which are configured separately in host {<server_fqdn> <server_ipv4> <host_pattern>}.</p> <p>Like host, this field supports back references such as \$0 to the parts reg-exp <object_pattern> for each object in the condition table.</p> <p>For an example, see the FortiWeb Administration Guide.</p>	No default.
url-status {enable disable}	<p>Enable to rewrite the URL part of the request URL.</p> <p>If you disable this option, the FortiWeb appliance preserves the value from the client's request when it rewrites it.</p> <p>This option is available only when action is http-header-rewrite.</p>	disable
location <location_str>	<p>Enter the replacement value for the Location: field in the HTTP header for the 302 response. The maximum length is 255 characters.</p> <p>This option is available only when action is redirect.</p>	No default.
location_replace <location_str>	<p>Type the URL string that provides a location for use in a 302 HTTP redirect response from a web server connected to FortiWeb. The maximum length is 255 characters.</p> <p>This option is available only when action is location-rewrite.</p>	No default.
referer-status {enable disable}	<p>Enable to rewrite the Referer: field in the HTML header. Also configure referer <referer-url_str> and referer-use-pserver {enable disable}.</p>	disable
referer <referer-url_str>	<p>Type the replacement value for the Referer: field in the HTML header. The maximum length is 255 characters.</p> <p>This option is available only when referer-status is enabled.</p>	No default.
referer-use-pserver {enable disable}	<p>Enable this when you have a server farm for server balance or content routing. In this case you do not know which server in the server farm the FortiWeb appliance will use. When FortiWeb processes the request, it sets the value for the actual referer.</p> <p>This option is available only when referer-status is enabled and action is http-header-rewrite. Any setting you make for referer is ignored.</p>	disable
body_replace <replacement_str>	<p>Type the value that will replace matching HTTP content in the body of responses. The maximum is 255 characters.</p> <p>For an example, see the FortiWeb Administration Guide.</p> <p>This option is available only when action is http-body-rewrite.</p>	No default.

Variable	Description	Default
<code><entry_index></code>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
<code>content-filter {enable disable}</code>	Enable if you want to match this condition only for specific HTTP content types (also called Internet or MIME file types) such as <code>text/html</code> , as indicated in the <code>Content-Type: HTTP</code> header. Also configure <code>content-type-set {text/html text/plain text/javascript application/xml (or) text/xml application/javascript application/soap+xml application/x-javascript}</code> .	disable
<code>content-type-set {text/html text/plain text/javascript application/xml (or) text/xml application/javascript application/soap+xml application/x-javascript}</code>	Type the HTTP content types that you want to match in a space-delimited list, such as: <code>set content-type-set text/html text/plain</code>	No default.
<code>HTTP-protocol {http https}</code>	Select which protocol will match this condition, either HTTP or HTTPS. This option is applicable only if <code>protocol-filter</code> is set to enable.	http
<code>is-essential {yes no}</code>	Select what to do if there is no <code>Referer:</code> field, either: <ul style="list-style-type: none"> no — Meet this condition. yes — Do not meet this condition. Requests can lack a <code>Referer:</code> field for several reasons, such as if the user manually types the URL, and the request does not result from a hyperlink from another web site, or if the URL resulted from an HTTPS connection. (See the RFC 2616 section on the <code>Referer:</code> field.) In those cases, the field cannot be tested for a matching value. This option appears only if <code>object</code> is <code>http-reference</code> .	yes
<code>object {http-host http-reference http-url}</code>	Select which part of the HTTP request to test for a match: <ul style="list-style-type: none"> http-host http-url http-reference (the <code>Referer:</code> field) If the request must match multiple conditions (for example, it must contain both a matching <code>Host:</code> field and a matching URL), add each object match condition to the condition table separately.	http-host

Variable	Description	Default
<code>protocol-filter {enable disable}</code>	<p>Enable if you want to match this condition only for either HTTP or HTTPS. Also configure HTTP-protocol {http https}.</p> <p>For example, you could redirect clients that accidentally request the login page by HTTP to a more secure HTTPS channel — but the redirect is not necessary for HTTPS requests.</p> <p>As another example, if URLs in HTTPS requests should be exempt from rewriting, you could configure the rewriting rule to apply only to HTTP requests.</p>	disable
<code>reg-exp <object_pattern></code>	<p>Depending on your selection in object {http-host http-reference http-url} and <code>reverse-match {yes no}</code>, type a regular expression that defines either all matching or all non-matching <code>Host:</code> fields, URLs, or <code>Referer:</code> fields. Then, also configure <code>reverse-match {yes no}</code>.</p> <p>For example, for the URL rewriting rule to match all URLs that begin with <code>/wordpress</code>, you could enter <code>^/wordpress</code>, then, in <code>reverse-match {yes no}</code>, select <code>no</code>.</p> <p>The pattern is not required to begin with a slash (<code>/</code>). The maximum length is 255 characters.</p> <p>Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported. Instead, use <code>reverse-match {yes no}</code>.</p>	No default.
<code>reverse-match {yes no}</code>	<p>Indicate how to use reg-exp <object_pattern> when determining whether or not this URL rewriting condition has been met.</p> <ul style="list-style-type: none"> <code>no</code> — If the regular expression does match the request object, the condition is met. <code>yes</code> — If the regular expression does not match the request object, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (<code>!</code>). <p>If all conditions are met, the FortiWeb appliance will do your selected <code>action</code>.</p>	no

Related topics

- [config waf url-rewrite url-rewrite-policy](#)

waf web-protection-profile autolearning-profile

Use this command to configure auto-learning profiles.

Auto-learning profiles are useful when you want to collect information about the HTTP sessions on your unique network in order to design inline or offline protection profiles suited for them. This reduces much of the research and guesswork about what HTTP request methods, data types, and other types of content that your web sites and web applications use when designing an appropriate defense.

Auto-learning profiles track your web servers' response to each request, such as 401 Unauthorized or 500 Internal Server Error, to learn about whether the request is legitimate or a potential attack attempt. Such data is used for auto-learning reports, and can serve as the basis for generating inline protection or offline protection profiles.

Auto-learning profiles are designed to be used in conjunction with a protection or detection profile, which is used to detect attacks. Only if attacks are detected can the auto-learning profile accumulate auto-learning data and generate its report. As a result, auto-learning profiles require that you also select a protection or detection profile in the same policy.



Use auto-learning profiles with profiles whose `action` is `alert`.

If `action` is `alert_deny`, the FortiWeb appliance will reset the connection, preventing the auto-learning feature from gathering complete data on the session.

To apply auto-learning profiles, select them within a policy. For details, see [“config waf web-protection-profile offline-protection” on page 406](#). Once applied in a policy, the FortiWeb appliance will collect data and generate a report from it. For details, see the [FortiWeb Administration Guide](#).

Before configuring an auto-learning profile, first configure any of the following that you want to include in the profile:

- a data type group (see [“config server-policy pattern data-type-group” on page 130](#))
- a suspicious URL rule group (see [“config server-policy pattern suspicious-url-rule” on page 137](#))
- a URL interpreter (see [“config server-policy custom-application application-policy” on page 108](#))



Alternatively, you could generate an auto-learning profile and its required components, and then modify them. For details, see the [FortiWeb Administration Guide](#).

You must also disable any globally whitelisted objects. (These will be exempt from scans and autolearning data.) See [“config server-policy pattern custom-global-white-list-group” on page 125](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `learngrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf web-protection-profile autolearning-profile
```

```

edit <auto-learning-profile_name>
    set data-type-group <data-type-group_name>
    set suspicious-url-rule <suspicious-url-rule-group_name>
    set attack-count-threshold <count_int>
    set attack-percent-range <percent_int>
    set application-policy <policy_name>
next
end

```

Variable	Description	Default
<auto-learning-profile_name>	Type the name of the auto-learning profile. The maximum length is 35 characters. To display the list of existing profile, type: edit ?	No default.
data-type-group <data-type-group_name>	Type the name of the data type group for the profile to use. See “config server-policy pattern data-type-group” on page 130 . The maximum length is 35 characters. To display the list of existing groups, type: set data-type-group ? The auto-learning profile will learn about the names, length, and required presence of these types of parameter inputs as described in the data type group.	No default.
suspicious-url-rule <suspicious-url-rule-group_name>	Type the name of a suspicious URL rule group to use. See “config server-policy pattern suspicious-url-rule” on page 137 . The maximum length is 35 characters. To display the list of existing groups, type: set suspicious-url-rule ? The auto-learning profile will learn about attempts to access URLs that are typically used for web server or web application administrator logins, such as <code>admin.php</code> . Requests from clients for these types of URLs are considered to be a possible attempt at either vulnerability scanning or administrative login attacks, and therefore potentially malicious.	No default.
attack-count-threshold <count_int>	Type the integer representing the threshold over which the auto-learning profile adds the attack to the server protection rules. The valid range is from 1 to 2,147,483,647.	100
attack-percent-range <percent_int>	Type the integer representing the threshold of the percentage of attacks to total hits over which the auto-learning profile adds the attack to the server protection exceptions. The valid range is from 1 to 10,000.	5
application-policy <policy_name>	Type the name of a custom application policy to use. See “config server-policy custom-application application-policy” on page 108 . The maximum length is 35 characters. To display the list of existing application policies, type: set application-policy ?	No default.

Related topics

- [config server-policy pattern custom-global-white-list-group](#)
- [config server-policy pattern data-type-group](#)
- [config server-policy pattern suspicious-url-rule](#)
- [config waf web-protection-profile inline-protection](#)
- [config server-policy policy](#)
- [config system settings](#)

waf web-protection-profile inline-protection

Use this command to configure inline protection profiles.

Inline protection profiles are a set of attack protection settings. The FortiWeb appliance applies the profile when a connection matches a server policy that includes the protection profile. You can use inline protection profiles in server policies for any mode except offline protection.

To apply protection profiles, select them within a server policy. For details, see [“config server-policy policy” on page 140](#).

Before configuring an inline protection profile, first configure any of the following that you want to include in the profile:

- a parameter validation rule (see [“config waf parameter-validation-rule” on page 353](#))
- start pages (see [“config waf start-pages” on page 368](#))
- caching of back-end server responses (see [“config waf web-cache-policy” on page 403](#))
- a URL access policy (see [“config waf url-access url-access-policy” on page 372](#))
- a hidden field rule group (see [“config waf hidden-fields-protection” on page 301](#))
- a parameter restriction constraint (see [“config waf http-protocol-parameter-restriction” on page 319](#))
- an authentication policy and/or site publisher (see [“config waf http-authen http-authen-policy” on page 307](#) or [“config waf site-publish-helper policy” on page 362](#))
- a brute force login attack sensor (see [“config waf brute-force-login” on page 269](#))
- an allowed method exception (see [“config waf allow-method-exceptions” on page 260](#))
- a list of manually trusted and black-listed IPs, FortiGuard IP reputation category-based blacklisted IPs, and/or a geographically-based IP blacklist (see [“config waf ip-intelligence” on page 332](#), [“config waf ip-list” on page 336](#) and [“config waf geo-block-list” on page 299](#))
- a page order rule (see [“config waf page-access-rule” on page 350](#))
- attack signatures (see [“config waf signature” on page 355](#))
- a file upload restriction policy (see [“config waf file-upload-restriction-policy” on page 292](#))
- a URL rewriting policy (see [“config waf url-rewrite url-rewrite-policy” on page 379](#))
- a DoS protection policy (see [“config waf application-layer-dos-prevention” on page 265](#))
- compression rules (see [“config waf file-compress-rule” on page 288](#))
- decompression rules ([“config waf file-uncompress-rule” on page 290](#))
- a policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS ([“config waf padding-oracle” on page 345](#))

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf web-protection-profile inline-protection
```

```

edit <inline-protection-profile_name>
  set http-session-management {enable | disable}
  set amf3-protocol-detection {enable | disable}
  set xml-protocol-detection {enable | disable}
  set malformed-xml-block-period <block-period_int>
  set malformed-xml-check {enable | disable}
  set malformed-xml-check-action {alert | alert_deny | block-
period}
  set malformed-xml-check-severity {High | Low | Medium}
  set malformed-xml-check-trigger <trigger-policy_name>
  [set custom-access-policy <combo-access_name>]
  [set brute-force-login <sensor_name>]
  set cookie-poison {enable | disable}
  set cookie-poison-action {alert | alert_deny | block-period |
remove_cookie}
  set cookie-poison-severity {High | Medium | Low}
  [set cookie-poison-trigger <trigger-policy_name>]
  set block-period <seconds_int>
  [set file-upload-policy <policy_name>]
  [set geo-block-list-policy <policy_name>]
  [set hidden-fields-protection <group_name>]
  [set http-authen-policy <policy_name>]
  [set http-protocol-parameter-restriction <constraint_name>]
  set http-session-timeout <seconds_int>
  [set ip-list-policy <policy_name>]
  [set known-search-engine {enable | disable}]
  [set padding-oracle <rule_name>]
  [set page-access-rule <rule_name>]
  [set parameter-validation-rule <rule_name>]
  [set redirect-url <redirect_fqdn>]
  set signature-rule {"High Level Security" | "Medium Level
Security" | "Alert Only" | <signature-set_name>}
  set rdt-reason {enable | disable}
  [set site-publisher-helper <policy_name>]
  [set start-pages <rule_name>]
  [set web-cache-policy <web-cache-policy_name>]
  [set ip-intelligence {enable | disable}]
  [set url-rewrite-policy <group_name>]
  [set url-access-policy <policy_name>]
  [set file-compress-rule <rule_name>]
  [set file-uncompress-rule <rule_name>]
  [set application-layer-dos-prevention <policy_name>]
  set data-analysis {enable | disable}
  set x-forwarded-for-rule <x-forwarded-for_name>

```

```

next
end

```

Variable	Description	Default
<code><inline-protection-profile_name></code>	Type the name of the inline protection profile. The maximum length is 35 characters. To display the list of existing profile, type: <code>edit ?</code>	No default.
<code>allow-method-policy <policy_name></code>	Type the name of an allowed method policy. See “config waf allow-method-policy” on page 263 . The maximum length is 35 characters. To display the list of existing policies, type: <code>set allow-method-policy ?</code>	No default.
<code>amf3-protocol-detection {enable disable}</code>	Enable to scan requests that use action message format 3.0 (AMF3) for <ul style="list-style-type: none"> • cross-site scripting (XSS) attacks • SQL injection attacks • common exploits if you have enabled those in the signature set specified by <code>signature-rule {"High Level Security" "Medium Level Security" "Alert Only" <signature-set_name>}</code> . AMF3 is a binary format that Adobe Flash clients can use to send input to server-side software. Caution: To scan for attacks or enforce input rules on AMF3, you must enable this option. Failure to enable the option will make the FortiWeb appliance unable to scan AMF3 requests for attacks.	disable
<code>xml-protocol-detection {enable disable}</code>	Enable to scan for matches with attack and data leak signatures in Web 2.0 (XML AJAX) and other XML submitted by clients in the bodies of HTTP POST requests.	disable
<code>malformed-xml-block-period <block-period_int></code>	Type the length of time that FortiWeb blocks XML traffic that contains malformed XML, in seconds. The valid range is from 1 to 3,600 seconds.	60
<code>malformed-xml-check {enable disable}</code>	Enable to validate that XML elements and attributes in the request's body conforms to the W3C XML 1.1 and/or XML 2.0 standards. Malformed XML, such as without the final > or with multiple >> in the closing tag, is often an attempt to exploit an unhandled error condition in a web application's XHTML or XML parser. This feature is applicable only when <code>xml-protocol-detection</code> is enable. Attack log messages contain Illegal XML Format when this feature detects malformed XML.	disable

Variable	Description	Default
malformed-xml-check-action {alert alert_deny block-period}	Specify the action that FortiWeb takes when it detects a request that contains malformed XML: <ul style="list-style-type: none"> alert — Accept the request and generate an alert email, a log message, or both. alert_deny — Block the request and generate an alert email, a log message, or both. block-period — Block the XML traffic for a number of seconds. Also configure <code>malformed-xml-block-period <block-period_int></code>. 	alert
malformed-xml-check-severity {High Low Medium}	Select the severity level to use in logs and reports generated when illegal XML formats are detected.	High
malformed-xml-check-trigger <trigger-policy_name>	Type the name of the trigger to apply when illegal XML formats are detected (see “ config log trigger-policy ” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
custom-access-policy <combo-access_name>	Type the name of a custom access policy. See “ config waf custom-access-policy ” on page 272. The maximum length is 35 characters. To display the list of existing policies, type: set custom-access-policy ?	No default.
brute-force-login <sensor_name>	Type the name of a brute force login attack sensor. See “ config waf brute-force-login ” on page 269. The maximum length is 35 characters. To display the list of existing sensors, type: set brute-force-login ?	No default.
cookie-poison {enable disable}	Enable to detect cookie poisoning. When enabled, each cookie is accompanied by a cookie named <code><cookie_name>_fortinet_waf_auth</code> , which tracks the cookie's original value when set by the web server. If the cookie returned by the client does not match this digest, the FortiWeb appliance will detect cookie poisoning.	disable

Variable	Description	Default
<pre>cookie-poison-action {alert alert_deny block-period remove_cookie}</pre>	<p>Select one of the following actions that the FortiWeb appliance will perform when it detects cookie poisoning:</p> <ul style="list-style-type: none"> • <code>alert</code> — Accept the request and generate an alert email and/or log message. • <code>alert_deny</code> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See the FortiWeb Administration Guide or <code>error-msg <message_str></code> in “server-policy policy” on page 140. • <code>block-period</code> — Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code>. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you <i>must</i> also define an X-header that indicates the original client’s IP (see “waf x-forwarded-for” on page 413). Failure to do so may cause FortiWeb to block <i>all</i> connections when it detects a violation of this type. • <code>remove_cookie</code> — Accept the request, but remove the poisoned cookie from the datagram before it reaches the web server, and generate an alert and/or log message. <p>Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> is enabled.</p> <p>Note: Logging and/or alert email will occur only if enabled and configured. See “config log disk” on page 70 and “config log alertemail” on page 64.</p> <p>Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 387.</p>	No default.
<pre>cookie-poison-severity {High Medium Low}</pre>	Select the severity level to use in logs and reports generated when cookie poisoning is detected.	High
<pre>block-period <seconds_int></pre>	Type the number of seconds to block a connection when <code>cookie-poison-action</code> is set to <code>block-period</code> . The valid range is from 1 to 3,600 seconds.	1

Variable	Description	Default
cookie-poison-trigger <trigger-policy_name>	Type the name of the trigger to apply when cookie poisoning is detected (see “config log trigger-policy” on page 99). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
file-upload-policy <policy_name>	Type the name of a file upload restriction policy to use, if any. See “config waf file-upload-restriction-policy” on page 292 . The maximum length is 35 characters. To display the list of existing policies, type: set file-upload-policy ?	No default.
geo-block-list-policy <policy_name>	Type the name of a geographically-based client IP black list that you want to apply, if any. See “config waf geo-block-list” on page 299 . The maximum length is 35 characters. To display the list of existing group, type: set geo-block-list-policy ?	No default.
hidden-fields-protection <group_name>	Type the name of a hidden field rule group that you want to apply, if any. See “config waf hidden-fields-protection” on page 301 . The maximum length is 35 characters. To display the list of existing group, type: set hidden-fields-protection ?	No default.
http-authen-policy <policy_name>	Type the name of an HTTP authentication policy, if any, that will be applied to matching HTTP requests. See “config waf http-authen http-authen-policy” on page 307 . The maximum length is 35 characters. To display the list of existing profile, type: set http-authen-policy ? If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.	No default.
http-protocol-parameter-restriction <constraint_name>	Type the name of an HTTP protocol constraint that you want to apply, if any. See “config waf http-protocol-parameter-restriction” on page 319 . The maximum length is 35 characters. To display the list of existing profile, type: set http-protocol-parameter-restriction ?	No default.

Variable	Description	Default
http-session-management {enable disable}	<p>Enable to add an implementation of HTTP sessions, and track their states, using a cookie such as <code>cookiesession1</code>. Also configure <code>http-session-timeout <seconds_int></code>.</p> <p>Although HTTP has no inherent support for sessions, a notion of individual HTTP client sessions, rather than simply the source IP address and/or timestamp, is required by some features.</p> <p>For example, you might want to require that a client's first HTTP request always be a login page: the rest of the web pages should be inaccessible if they have not authenticated. Out-of-order requests could represent an attempt to bypass the web application's native authentication mechanism. How can FortiWeb know if a request is the client's first HTTP request? If FortiWeb were to treat each request independently, without knowledge of anything previous, it could not, by definition, enforce page order. Therefore FortiWeb must keep some record of the first request from that client (the session initiation). It also must record their previous HTTP request(s), until a span of time (the session timeout) has elapsed during which there were no more subsequent requests, after which it would require that the session be initiated again.</p> <p>The session management feature provides such FortiWeb session support.</p> <p>This feature requires that the client support cookies.</p> <p>Note: You <i>must</i> enable this option:</p> <ul style="list-style-type: none"> to enforce the start page rule, page access rule, and hidden fields rule, if any of those are selected. if you want to include this profile's traffic in the traffic log, in addition to enabling traffic logs in general. For more information, see “config log attack-log” on page 65 and “config log memory” on page 81. 	disable
http-session-timeout <seconds_int>	<p>Type the HTTP session timeout in seconds. The valid range is from 20 to 1,200 seconds.</p> <p>This setting is available only if <code>http-session-management</code> is enabled.</p>	1200
ip-list-policy <policy_name>	<p>Type the name of a trusted IP or blacklisted IP policy. See “config waf ip-list” on page 336. The maximum length is 35 characters.</p> <p>To display the list of existing policy, type:</p> <pre>set ip-list-policy ?</pre>	No default.

Variable	Description	Default
known-search-engine {enable disable}	<p>Enable to allow or block predefined search engines, robots, spiders, and web crawlers according to your settings in the global list.</p> <p>Enable to exempt popular search engines' robots, spiders, and web crawlers from DoS sensors, brute force login sensors, HTTP protocol constraints, and combination rate & access control (called "advanced protection" and "custom policies" in the web UI).</p> <p>This option improves access for search engines. Rapid access rates, unusual HTTP usage, and other characteristics that may be suspicious for web browsers are often normal with search engines. If you block them, your web sites' rankings and visibility may be affected.</p> <p>By default, this option allows all popular predefined search engines. Known search engine indexer source IPs are updated via FortiGuard Security Service. To specify which search engines will be exempt, enable or disable each search engine in "server-policy pattern custom-global-white-list-group" on page 125.</p> <p>Note: X-header-derived client source IPs (see "waf x-forwarded-for" on page 413) do not support this feature in this release. If FortiWeb is deployed behind a load balancer or other web proxy that applies source NAT, this feature will not work.</p>	disable
padding-oracle <rule_name>	<p>Type the name of a padding oracle protection rule. See "config waf padding-oracle" on page 345. The maximum length is 35 characters.</p> <p>To display the list of existing rule, type:</p> <pre>set padding-oracle ?</pre>	No default.
page-access-rule <rule_name>	<p>Type the name of a page order rule. See "config waf page-access-rule" on page 350. The maximum length is 35 characters.</p> <p>To display the list of existing rule, type:</p> <pre>set page-access-rule ?</pre>	No default.
parameter-validation-rule <rule_name>	<p>Type the name of a parameter validation rule. See "config waf parameter-validation-rule" on page 353. The maximum length is 35 characters.</p> <p>To display the list of existing rule, type:</p> <pre>set parameter-validation-rule ?</pre>	No default.

Variable	Description	Default
<code>redirect-url</code> <code><redirect_fqdn></code>	<p>Type a URL including the FQDN/IP and path, if any, to which an HTTP client will be redirected if their HTTP request violates any of the rules in this profile.</p> <p>For example, you could enter <code>www.example.com/products/</code>.</p> <p>If you do not enter a URL, depending on the type of violation and the configuration, the FortiWeb appliance will log the violation, may attempt to remove the offending parts, and could either reset the connection or return an HTTP 403 (Access Forbidden) or 404 (File Not Found) error message.</p> <p>The maximum length is 255 characters.</p>	No default.
<code>signature-rule {"High Level Security" "Medium Level Security" "Alert Only" <signature-set_name>}</code>	<p>Specify a signature policy to include in the profile (see “config waf signature” on page 355).</p> <p>The maximum length is 35 characters.</p> <p>To display the list of existing rules, type:</p> <pre>set server-protection-rule ?</pre> <p>The type of attack that FortiWeb detects determines the attack log messages for this feature. For a list, see “config waf signature” on page 355.</p>	No default.
<code>rdt-reason {enable disable}</code>	<p>Enable to include the reason for URL redirection as a parameter in the URL, such as <code>reason=DETECT_PARAM_RULE_FAILED</code>, when traffic has been redirected using <code>redirect-url <redirect_fqdn></code>. The FortiWeb appliance also adds <code>fortiwaf=1</code> to the URL to detect and cancel a redirect loop (when the redirect action recursively triggers an attack event).</p> <p>Caution: If you specify a redirect URL that is protected by the FortiWeb appliance, you should enable this option to prevent infinite redirect loops.</p>	No default.
<code>site-publisher-helper</code> <code><policy_name></code>	<p>Type the name of a site publishing policy, if any, that will be applied to matching HTTP requests. See “config waf site-publish-helper policy” on page 362. The maximum length is 35 characters.</p> <p>To display the list of existing profile, type:</p> <pre>set site-publisher-policy ?</pre> <p>If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.</p>	No default.
<code>start-pages</code> <code><rule_name></code>	<p>Type the name of a start page rule. See “config waf start-pages” on page 368. The maximum length is 35 characters.</p> <p>To display the list of existing rule, type:</p> <pre>set start-pages ?</pre> <p>This setting is available only if <code>http-session-management</code> is enabled.</p>	No default.

Variable	Description	Default
web-cache-policy <web-cache-policy_name>	Type the name of content caching policy. See “config waf web-cache-policy” on page 403 . The maximum length is 35 characters. To display the list of existing policies, type: set web-cache-policy ?	No default.
ip-intelligence {enable disable}	Enable to apply intelligence about the reputation of the client's source IP. Blocking and logging behavior is configured in config waf ip-intelligence .	disable
url-rewrite-policy <group_name>	Type the name of a URL rewriting rule set, if any, that will be applied to matching HTTP requests. The maximum length is 35 characters. To display the list of existing policy, type: set url-rewrite-policy ? See “config waf url-access url-access-policy” on page 372 .	No default.
url-access-policy <policy_name>	Type the name of a url access policy. See “config waf url-access url-access-policy” on page 372 . The maximum length is 35 characters. To display the list of existing policy, type: set url-access-policy ?	No default.
file-compress-rule <rule_name>	Type the name of an existing file compression rule to use with this profile, if any. See “config waf file-compress-rule” on page 288 . The maximum length is 35 characters. To display the list of existing rule, type: set file-compress-rule ?	No default.
file-uncompress-rule <rule_name>	Type the name of an existing file uncompression rule to use with this profile, if any. See “config waf file-uncompress-rule” on page 290 . The maximum length is 35 characters. To display the list of existing rule, type: set file-uncompress-rule ?	No default.
application-layer-dos-prevention <policy_name>	Type the name of an existing DoS protection policy to use with this profile, if any. See “waf application-layer-dos-prevention” on page 265 . The maximum length is 35 characters. To display the list of existing profile, type: set application-layer-dos-prevention ?	No default.
data-analysis {enable disable}	Enable this to collect data for servers covered by this profile. To view the statistics for collected data, in the web UI, go to <i>Log&Report > Monitor > Data Analytics</i> .	disable
x-forwarded-for-rule <x-forwarded-for_name>	Specify the name of a rule that configures FortiWeb's use of X-Forwarded-For: and X-Real-IP (see “waf x-forwarded-for” on page 413).	No default.

Related topics

- [config log trigger-policy](#)
- [config server-policy pattern custom-global-white-list-group](#)
- [config server-policy policy](#)
- [config waf signature](#)
- [config waf start-pages](#)
- [config waf padding-oracle](#)
- [config waf page-access-rule](#)
- [config waf parameter-validation-rule](#)
- [config waf http-protocol-parameter-restriction](#)
- [config waf url-access url-access-policy](#)
- [config waf allow-method-exceptions](#)
- [config waf application-layer-dos-prevention](#)
- [config waf file-compress-rule](#)
- [config waf file-uncompress-rule](#)
- [config waf brute-force-login](#)
- [config waf geo-block-list](#)
- [config waf hidden-fields-protection](#)
- [config waf http-authen http-authen-policy](#)
- [config waf http-protocol-parameter-restriction](#)
- [config waf ip-intelligence](#)
- [config waf ip-list](#)
- [config waf web-cache-exception](#)
- [config waf web-cache-policy](#)

waf web-cache-exception

Use this command to configure FortiWeb to cache responses from your servers.

Use `web-cache-exception` to cache all URLs except for a few. To cache only a few URLs, see [“config waf web-cache-policy” on page 403](#).

To apply this policy, include it in an inline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf web-cache-exception
  edit <web-cache-exception_rule_name>
    config exception-list
      edit <entry_index>
        set host-status {enable | disable}
        set host <host_str>
        set url-type {plain | regular}
        set url-pattern <url-pattern_str>
        set cookie-name <cookie-name_str>
      end
    next
  end
```

Variable	Description	Default
<web-cache-exception_rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing policies, type: <code>edit ?</code>	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
host-status {enable disable}	Specify <code>enable</code> to require that the <code>Host:</code> field of the HTTP request match a protected host names entry in order to match the exception. Also specify a value for <code>host</code> .	disable
<host_str>	Specify which protected host names entry (either a web host name or IP address) that the <code>Host:</code> field of the HTTP request must be in to match the exception. Maximum length is 255 characters. This option is available only if the value of <code>host-status</code> is enabled.	No default.
{plain regular}	Specify the type of value that is used for <code>url-pattern</code> : <code>plain</code> — A literal URL. <code>regular</code> — A regular expression designed to match multiple URLs.	plain

Variable	Description	Default
<code><url-pattern_str></code>	<p>If the value of <code>url-type</code> is <code>plain</code>, specify the literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (<code>/</code>).</p> <p>If the value of <code>url-type</code> is <code>regular</code>, specify a regular expression, such as <code>^/*.php</code>, that matches all and only the URLs that the rule applies to. The pattern does not require a slash (<code>/</code>); however, it must match URLs that begin with a slash, such as <code>/index.cfm</code>.</p> <p>Do not include the domain name, such as <code>www.example.com</code>, which is specified by <code>host</code>.</p> <p>Maximum length is 255 characters.</p> <p>Tip: Generally, URLs that require autolearning adapters do not work well with caching either. Do not cache dynamic URLs that contain variables such as user names (e.g. older versions of Microsoft OWA) or volatile data such as parameters. Because FortiWeb is unlikely to receive identical subsequent requests for them, dynamic URLs can rapidly consume cache without improving performance.</p>	No default.
<code><cookie-name_str></code>	<p>Specify the name of the cookie, such as <code>sessionid</code>, as it appears in the <code>Cookie: HTTP</code> header.</p> <p>Maximum length is 127 characters.</p> <p>Tip: Content that is unique to a user, such as personalized pages that appear after a person has logged in, usually should not be cached. If the web application's authentication is cookie-based, configure this setting with the name of the authentication cookie. Otherwise, if it is parameter-based, configure the exception with a URL pattern that matches the authentication ID parameter.</p>	No default.

Related topics

- [config waf web-cache-policy](#)
- [config waf web-protection-profile inline-protection](#)

waf web-cache-policy

Use this command to configure FortiWeb to cache responses from your servers.

Use `web-cache-policy` to cache only a few URLs. To cache all URLs except for a few, see [“config waf web-cache-exception” on page 401](#).

To apply this policy, include it in an inline protection profile. For details, see [“config waf web-protection-profile inline-protection” on page 390](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf web-cache-policy
  edit <web-cache-policy_rule_name>
    set cache-buffer-size <cache-size_int>
    set max-cached-page-size <page-size_int>
    set default-cache-timeout <cache-timeout_int>
    set exception <web-cache-exception_name>
    config url-match-list
      edit <entry_index>
        set host-status {enable | disable}
        set host <host_str>
        set url-type {plain | regular}
        set url-pattern <url-pattern_str>
      end
    end
  end
```

next
end

Variable	Description	Default
<code><web-cache-policy_rule_name></code>	<p>Type the name of a new or existing rule. The maximum length is 35 characters.</p> <p>To display the list of existing policies, type:</p> <pre>edit ?</pre>	No default.
<code><cache-size_int></code>	<p>Specify the maximum amount of RAM to allocate to caching content, in MB (megabytes).</p> <p>You cannot store cached content on FortiWeb's hard disk.</p> <p>The FortiWeb model determines the valid range of values:</p> <ul style="list-style-type: none"> FortiWeb 400C, FortiWeb-VM (2-4 GB RAM) — 1-100 MB FortiWeb 1000C, FortiWeb-VM (4-8 GB RAM) — 1-200 MB FortiWeb 3000C, FortiWeb 3000C/CFsx, FortiWeb-VM (816 GB RAM)— 1-400 MB FortiWeb 4000C — 1-600 MB FortiWeb 1000D — 1-800 MB FortiWeb-VM (16+ GB RAM) — 1-1024 MB FortiWeb 3000D/DFsx — 1-1200 MB FortiWeb 4000D — 1-2048 MB <p>If administrative domains (ADOMs) are enabled, the maximums apply to the total RAM allotted to all ADOMs. For example, a FortiWeb 1000D has two ADOMs. If the <code>cache-buffer-size</code> value for the first ADOM is 600, the valid range for <code>cache-buffer-size</code> for the second ADOM is 1-200.</p> <p>Tip: For improved performance, adjust this setting until it is as small as possible yet FortiWeb can still fit most graphics and server processing-intensive pages into its cache. This allows FortiWeb to allocate more RAM to other features that also affect throughput, such as scanning for attacks.</p>	100
<code><page-size_int></code>	<p>Specify the maximum size of each URL that FortiWeb caches, in kilobytes (KB). FortiWeb does not cache objects such as high-resolution images, movies, or music that are larger than this value.</p> <p>Valid range is 1 to 10,240.</p> <p>Tip: For improved performance, adjust this setting until FortiWeb can fit most graphics and server processing-intensive pages into its cache.</p>	2048
<code><cache-timeout_int></code>	<p>Specify the time to live for each entry in the cache. FortiWeb removes expired entries.</p> <p>Valid range is 0 to 7200.</p> <p>When it receives a subsequent request for the URL, FortiWeb forwards the request to the server and refreshes the cached response. Any additional requests receive the new cached response until the URL's cache timeout expires.</p>	1440

Variable	Description	Default
<code><web-cache-exception_name></code>	Specify the name of a list of exceptions. See “config waf web-cache-exception” on page 401 .	No default.
<code><entry_index></code>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999.	No default.
<code>host-status {enable disable}</code>	Specify <code>enable</code> to require that the <code>Host:</code> field of the HTTP request match a protected host names entry in order to match the policy. Also specify a value for <code>host</code> .	disable
<code><host_str></code>	Specify which protected host names entry (either a web host name or IP address) that the <code>Host:</code> field of the HTTP request must be in to match the policy. This option is available only if the value of <code>host-status</code> is enabled.	No default.
<code>{plain regular}</code>	Specify the type of value that is used for <code>url-pattern</code> : <code>plain</code> — A literal URL. <code>regular</code> — A regular expression designed to match multiple URLs.	plain
<code><url-pattern_str></code>	If the value of <code>url-type</code> is <code>plain</code> , specify the literal URL, such as <code>/index.php</code> , that the HTTP request must contain in order to match the rule. The URL must begin with a slash (/). If the value of <code>url-type</code> is <code>regular</code> , specify a regular expression, such as <code>^/*.php</code> , that matches all and only the URLs that the rule applies to. The pattern does not require a slash (/); however, it must match URLs that begin with a slash, such as <code>/index.cfm</code> . Do not include the domain name, such as <code>www.example.com</code> , which is specified by <code>host</code> .	No default.

Related topics

- [config waf web-cache-exception](#)
- [config waf web-protection-profile inline-protection](#)

waf web-protection-profile offline-protection

Use this command to configure offline protection profiles.

Detection profiles are useful when you want to preview the effects of some web protection features without affecting traffic, or without affecting your network topology.

Unlike protection profiles, a detection profile is designed for use in offline protection mode. Detection profiles cannot be guaranteed to block attacks. They attempt to reset the connection, but due to variable speeds of different routing paths, the reset request may arrive after the attack has been completed. Their primary purpose is to detect attacks, especially for use in conjunction with auto-learning profiles. In fact, if used in conjunction with auto-learning profiles, you **should** configure the detection profile to log only and not block attacks in order to gather complete session statistics for the auto-learning feature. As a result, detection profiles can only be selected in policies whose `deployment-mode` is `offline-detection`, and those policies will only be used by the FortiWeb appliance when its operation mode is `offline-detection`.

Unlike inline protection profiles, offline protection profiles do not support HTTP conversion, cookie poisoning detection, start page rules, and page access rules.

To apply detection profiles, select them within a server policy. For details, see [“config server-policy policy” on page 140](#).

Before configuring an offline protection profile, first configure any of the following that you want to include in the profile:

- a file upload restriction policy (see [“config waf file-upload-restriction-policy” on page 292](#))
- a server protection rule (see [“config waf signature” on page 355](#))
- a list of manually trusted and black-listed IPs, FortiGuard IRIS category-based blacklisted IPs, and/or a geographically-based IP blacklist (see [“config waf ip-intelligence” on page 332](#), [“config waf ip-list” on page 336](#) and [“config waf geo-block-list” on page 299](#))
- a parameter validation rule (see [“config waf parameter-validation-rule” on page 353](#))
- a URL access policy (see [“config waf url-access url-access-policy” on page 372](#))
- an allowed method exception (see [“config waf allow-method-exceptions” on page 260](#))
- a hidden field rule group (see [“config waf hidden-fields-protection” on page 301](#))
- a parameter restriction constraint (see [“config waf http-protocol-parameter-restriction” on page 319](#))
- an authentication policy (see [“config waf http-authen http-authen-policy” on page 307](#))
- a brute force login attack sensor (see [“config waf brute-force-login” on page 269](#))
- a decompression rule (see [“config waf file-uncompress-rule” on page 290](#))
- a policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS ([“config waf padding-oracle” on page 345](#))

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config waf web-protection-profile offline-protection
```

```

edit <offline-protection-profile_name>
    [set allow-method-policy <policy_name>]
    set amf3-protocol-detection {enable | disable}
    set xml-protocol-detection {enable | disable}
    set malformed-xml-block-period <block-period_int>
    set malformed-xml-check {enable | disable}
    set malformed-xml-check-action {alert | alert_deny | block-
period}
    set malformed-xml-check-severity {High | Low | Medium}
    set malformed-xml-check-trigger <trigger-policy_name>
    [set file-upload-policy <policy_name>]
    [set geo-block-list-policy <policy_name>]
    [set http-session-keyword <key_str>]
    set http-session-management {enable | disable}
    set http-session-timeout <seconds_int>
    [set ip-list-policy <policy_name>]
    set ip-intelligence {enable | disable}
    set known-search-engine {enable | disable}
    [set padding-oracle <rule_name>]
    [set parameter-validation-rule <rule_name>]
    [set url-access-policy <policy_name>]
    [set signature-rule {"High Level Security" | "Medium Level
Security" | "Alert Only" | <signature-set_name>}]
    [set http-authen-policy <http-auth_name>]
    [set hidden-fields-protection <group_name>]
    [set http-protocol-parameter-restriction <constraint_name>]
    [set file-uncompress-rule <rule_name>]
    [set brute-force-login <sensor_name>]
    set custom-access-policy <combo-access_name>
    set data-analysis {enable | disable}
    set x-forwarded-for-rule <x-forwarded-for_name>
next
end

```

Variable	Description	Default
<offline-protection-profile_name>	Type the name of the offline protection profile. The maximum length is 35 characters. To display the list of existing profile, type: edit ?	No default.
allow-method-policy <policy_name>	Type the name of an allowed method policy. See “config waf allow-method-policy” on page 263 . The maximum length is 35 characters. To display the list of existing policies, type: set allow-method-policy ?	No default.

Variable	Description	Default
amf3-protocol-detection {enable disable}	<p>Enable to be able to scan requests that use action message format 3.0 (AMF3) for</p> <ul style="list-style-type: none"> • cross-site scripting (XSS) attacks • SQL injection attacks • common exploits <p>if you have enabled those in the set of signatures specified by <code>signature-rule {"High Level Security" "Medium Level Security" "Alert Only" <signature-set_name>}</code>.</p> <p>AMF3 is a binary format that can be used by Adobe Flash clients to send input to server-side software.</p> <p>Caution: To scan for attacks or enforce input rules on AMF3, you <i>must</i> enable this option. Failure to enable the option makes the FortiWeb appliance unable to scan AMF3 requests for attacks.</p>	disable
xml-protocol-detection {enable disable}	Enable to scan for matches with attack and data leak signatures in Web 2.0 (XML AJAX) and other XML submitted by clients in the bodies of HTTP POST requests.	disable
malformed-xml-block-period <block-period_int>	<p>Type the length of time that FortiWeb blocks XML traffic that contains malformed XML, in seconds.</p> <p>The valid range is from 1 to 3,600 seconds.</p>	60
malformed-xml-check {enable disable}	<p>Enable to validate that XML elements and attributes in the request's body conforms to the W3C XML 1.1 and/or XML 2.0 standards. Malformed XML, such as without the final > or with multiple >> in the closing tag, is often an attempt to exploit an unhandled error condition in a web application's XHTML or XML parser.</p> <p>This feature is applicable only when <code>xml-protocol-detection</code> is enable. Attack log messages contain Illegal XML Format when this feature detects malformed XML.</p>	disable
malformed-xml-check-action {alert alert_deny block-period}	<p>Specify the action that FortiWeb takes when it detects a request that contains malformed XML:</p> <ul style="list-style-type: none"> • alert — Accept the request and generate an alert email, a log message, or both. • alert_deny — Block the request and generate an alert email, a log message, or both. • block-period — Block the XML traffic for a number of seconds. Also configure <code>malformed-xml-block-period <block-period_int></code>. 	alert
malformed-xml-check-severity {High Low Medium}	Select the severity level to use in logs and reports generated when illegal XML formats are detected.	High

Variable	Description	Default
malformed-xml-check-trigger <trigger-policy_name>	<p>Type the name of the trigger to apply when illegal XML formats are detected (see “config log trigger-policy” on page 99).</p> <p>The maximum length is 35 characters.</p> <p>To display the list of existing trigger policies, type:</p> <pre>set trigger ?</pre>	No default.
file-upload-policy <policy_name>	<p>Type the name of a file upload restriction policy. See “config waf file-upload-restriction-policy” on page 292. The maximum length is 35 characters.</p> <p>To display the list of existing policy, type:</p> <pre>set file-upload-policy ?</pre>	No default.
geo-block-list-policy <policy_name>	<p>Type the name of a geographically-based client IP black list that you want to apply, if any. See “config waf geo-block-list” on page 299. The maximum length is 35 characters.</p> <p>To display the list of existing group, type:</p> <pre>set geo-block-list-policy ?</pre>	No default.
http-session-keyword <key_str>	<p>If you want to use an HTTP header other than Session-Id: to track separate HTTP sessions, enter the key portion of the HTTP header that you want to use, such as Session-Num.</p> <p>The maximum length is 35 characters.</p>	No default.

Variable	Description	Default
http-session-management {enable disable}	<p>Enable to track the states of HTTP sessions. Also configure http-session-timeout <seconds_int>.</p> <p>Although HTTP has no inherent support for sessions, a notion of individual HTTP client sessions, rather than simply the source IP address and/or timestamp, is required by some features.</p> <p>For example, you might want to require that a client's first HTTP request always be a login page: the rest of the web pages should be inaccessible if they have not authenticated. Out-of-order requests could represent an attempt to bypass the web application's native authentication mechanism. How can FortiWeb know if a request is the client's first HTTP request? If FortiWeb were to treat each request independently, without knowledge of anything previous, it could not, by definition, enforce page order. Therefore FortiWeb must keep some record of the first request from that client (the session initiation). It also must record their previous HTTP request(s), until a span of time (the session timeout) has elapsed during which there were no more subsequent requests, after which it would require that the session be initiated again.</p> <p>The session management feature provides such FortiWeb session support.</p> <p>Note: This feature requires that the client support cookies.</p> <p>Note: You <i>must</i> enable this option if you want to include this profile's traffic in the traffic log, in addition to enabling traffic logs in general. For more information, see "config log attack-log" on page 65 and "config log memory" on page 81.</p>	disable
http-session-timeout <seconds_int>	<p>Type the HTTP session timeout in seconds. The valid range is from 20 to 1,200 seconds.</p> <p>This setting is available only if <code>http-session-management</code> is enabled.</p>	1200
ip-list-policy <policy_name>	<p>Type the name of a trusted IP or blacklisted IP policy. See "config waf ip-list" on page 336. The maximum length is 35 characters.</p> <p>To display the list of existing policy, type:</p> <pre>set ip-list-policy ?</pre>	No default.
ip-intelligence {enable disable}	<p>Enable to apply intelligence about the reputation of the client's source IP. Blocking and logging behavior is configured in config waf ip-intelligence.</p>	disable
known-search-engine {enable disable}	<p>Enable to allow or block predefined search engines, robots, spiders, and web crawlers according to your settings in the global list.</p>	disable

Variable	Description	Default
padding-oracle <rule_name>	Type the name of a padding oracle protection rule. See “config waf padding-oracle” on page 345 . The maximum length is 35 characters. To display the list of existing rule, type: set padding-oracle ?	No default.
parameter-validation-rule <rule_name>	Type the name of a parameter validation rule. See “config waf parameter-validation-rule” on page 353 . The maximum length is 35 characters. To display the list of existing rule, type: set parameter-validation-rule ?	No default.
url-access-policy <policy_name>	Type the name of a URL access policy. See “config waf url-access url-access-policy” on page 372 . The maximum length is 35 characters. To display the list of existing policy, type: set url-access-policy ?	No default.
signature-rule {"High Level Security" "Medium Level Security" "Alert Only" <signature-set_name>}	Specify a signature policy to include in the profile (see “config waf signature” on page 355). The maximum length is 35 characters. To display the list of existing rules, type: set server-protection-rule ? The type of attack that FortiWeb detects determines the attack log messages for this feature. For a list, see “config waf signature” on page 355 .	No default.
http-authen-policy <http-auth_name>	Type the name of an HTTP authentication policy, if any, that will be applied to matching HTTP requests. See “config waf http-authen http-authen-policy” on page 307 . The maximum length is 35 characters. To display the list of existing policies, type: set http-authen-policy ? If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.	No default.
hidden-fields-protection <group_name>	Type the name of a hidden field rule group that you want to apply, if any. See “config waf hidden-fields-protection” on page 301 . The maximum length is 35 characters. To display the list of existing group, type: set hidden-fields-protection ?	No default.
http-protocol-parameter-restriction <constraint_name>	Type the name of an HTTP protocol constraint that you want to apply, if any. See “config waf http-protocol-parameter-restriction” on page 319 . The maximum length is 35 characters. To display the list of existing constraint, type: set http-protocol-parameter-restriction ?	No default.

Variable	Description	Default
file-uncompress-rule <rule_name>	Type the name of an existing file decompression rule to use with this profile, if any. See “config waf file-uncompress-rule” on page 290 . The maximum length is 35 characters. To display the list of existing rule, type: set file-uncompress-rule ?	No default.
brute-force-login <sensor_name>	Type the name of a brute force login attack sensor. See “config waf brute-force-login” on page 269 . The maximum length is 35 characters. To display the list of existing sensor, type: edit ?	No default.
custom-access-policy <combo-access_name>	Type the name of a custom access policy. See “config waf custom-access policy” on page 272 . The maximum length is 35 characters. To display the list of existing policies, type: set custom-access-policy ?	No default.
data-analysis {enable disable}	Enable this to collect data for servers covered by this profile. To view the statistics for collected data, in the web UI, go to <i>Log&Report > Monitor > Data Analytics</i> .	disable
x-forwarded-for-rule <x-forwarded-for_name>	Specify the name of a rule that configures FortiWeb’s use of X-Forwarded-For: and X-Real-IP (see “waf x-forwarded-for” on page 413).	No default.

Related topics

- [config server-policy policy](#)
- [config waf signature](#)
- [config waf padding-oracle](#)
- [config waf parameter-validation-rule](#)
- [config waf url-access url-access-rule](#)
- [config waf allow-method-exceptions](#)
- [config system settings](#)
- [config waf file-uncompress-rule](#)
- [config waf brute-force-login](#)
- [config waf geo-block-list](#)
- [config waf hidden-fields-protection](#)
- [config waf http-authen http-authen-policy](#)
- [config waf http-protocol-parameter-restriction](#)
- [config waf ip-intelligence](#)
- [config waf ip-list](#)

waf x-forwarded-for

Use this command to configure FortiWeb's use of X-Forwarded-For: and X-Real-IP:.

For behavior of this feature and requirements, see the [FortiWeb Administration Guide](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config waf x-forwarded-for
  edit <x-forwarded-for_name>
    set block-based-on-original-ip {enable | disable}
    set ip-location {left | right}
    set original-ip-header <http-header-key_str>
    set tracing-original-ip {enable | disable}
    set x-forwarded-proto {enable | disable}
    set x-forwarded-for-support {enable | disable}
    set x-real-ip {enable | disable}
  config ip-list
    edit <entry_index>
      set ip <load-balancer_ip>
    next
  end
next
end
```

Variable	Description	Default
<x-forwarded-for_name>	Type the name of the new or existing group. The maximum length is 35 characters. To display the list of existing groups, type: <code>edit ?</code>	No default.
block-based-on-original-ip {enable disable}	Enable to be able to block requests that violate your policies by using the original client's IP derived from this HTTP X-header. When disabled, only attack logs and reports will use the original client's IP.	disable
ip-location {left right}	Select whether to extract the original client's IP from either the left or right end of the HTTP X-header line. Most proxies put the request's origin at the left end, which is the default setting. Some proxies, however, place it on the right end.	left
original-ip-header <http-header-key_str>	Type the key such as X-Forwarded-For X-Real-IP, without the colon (:), of the X-header that contains the original source IP address of the client. Also configure <code>tracing-original-ip {enable disable}</code> and, for security reasons, <code>ip <load-balancer_ip></code> . Maximum length is 255 characters.	No default.

Variable	Description	Default
tracing-original-ip {enable disable}	<p>If FortiWeb is deployed behind a device that applies NAT, enable this option to derive the original client's source IP address from an HTTP X-header, instead of the SRC field in the IP layer. Also configure original-ip-header <http-header-key_str> and, for security reasons, ip <load-balancer_ip>.</p> <p>This HTTP header is often X-Forwarded-For: when traveling through a web proxy, but can vary. For example, the Akamai service uses True-Client-IP:.</p> <p>For deployment guidelines and mechanism details, see the FortiWeb Administration Guide.</p> <p>Caution: To combat forgery, configure the IP addresses of load balancers and proxies that are trusted providers of this header. Also configure those proxies/load balancers to reject fraudulent headers, rather than passing them to FortiWeb.</p>	disable
x-forwarded-proto {enable disable}	<p>Enable to add an X-Forwarded-Proto: header that indicates the protocol used in the client's original request.</p> <p>Requires reverse proxy mode or true transparent proxy.</p>	disable
x-forwarded-for-support {enable disable}	<p>Enable to include the X-Forwarded-For: HTTP header on requests forwarded to your web servers. Behavior varies by the header already provided by the HTTP client or web proxy, if any.</p> <ul style="list-style-type: none"> • Header absent — Add the header, using the source IP address of the connection. • Header present — Verify that the source IP address of the connection is present in this header's list of IP addresses. If it is not, append it. <p>This option can be useful for web servers that log or analyze clients' IP addresses, and support the X-Forwarded-For: header. When this option is disabled, from the web server's perspective, all connections appear to be coming from the FortiWeb appliance, which performs network address translation (NAT). But when enabled, the web server can instead analyze this header to determine the source and path of the original client connection.</p> <p>This option applies only when FortiWeb is operating in reverse proxy mode or true transparent proxy.</p>	disable

Variable	Description	Default
x-real-ip {enable disable}	<p>Enable to include the X-Real-IP: HTTP header on requests forwarded to your web servers. Behavior varies by the header already provided by the HTTP client or web proxy, if any (see x-forwarded-for-support {enable disable}).</p> <p>Like X-Forwarded-For:, this header is also used by some proxies and web servers to trace the path, log, or analyze based upon the packet's original source IP address.</p> <p>This option applies only when FortiWeb is operating in reverse proxy mode or true transparent proxy.</p>	disable
x-forwarded-proto {enable disable}	<p>Enable to add an HTTP header that indicates the service used in the client's original request.</p> <p>Usually if your FortiWeb is receiving HTTPS requests from clients, and it is operating in reverse proxy mode, SSL/TLS is being offloaded. FortiWeb has terminated the SSL/TLS connection and the second segment of the request, where it forwards to the back-end servers, is clear text HTTP. In some cases, your back-end server may need to know that the original request was, in fact, encrypted HTTPS, not HTTP.</p>	disable
<entry_index>	<p>Type the index number of the individual entry in the table.</p> <p>The valid range is from 1 to 9,223,372,036,854,775,807.</p> <p>Each list can contain a maximum of 256 IP addresses.</p>	No default.
ip <load-balancer_ip>	<p>Type the IP address of a load balancer or proxy that is in front of the FortiWeb appliance (between the client and FortiWeb).</p> <p>To apply anti-spoofing measures and improve security, FortiWeb will trust the contents of the HTTP header that you specified in original-ip-header <http-header-key_str> only if the packet arrived from one of the IP addresses you specify here. Other packets' original-ip-header <http-header-key_str> will be regarded as potentially spoofed.</p>	No default.

Example

```
config waf x-forwarded-for
  edit "load-balancer1"
    set x-forwarded-for-support enable
    set tracing-original-ip enable
    set original-ip-header X-FORWARDED-FOR
    set x-real-ip enable
    set x-forwarded-proto enable
```

```
config ip-list
  edit 1
    set ip 192.168.1.105
  next
end
set block-based-on-original-ip enable
next
end
```


wvs policy

Use this command to define a web vulnerability scan policy. The policy enables you to set the frequency of the vulnerability scan, schedule the scan, and choose a format for the scan report. The policy also enables you to select an email policy that determines who receives the scan report.

Before you can complete a web vulnerability scan policy, you must first configure a scan profile using the FortiWeb web UI and a scan schedule using either the web UI or the command [config wvs schedule](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
config wvs policy
  edit <wvs-policy_name>
    set type {runonce | schedule}
    set schedule <wvs-schedule_name>
    set profile <wvs-profile_name>
    set email <email-policy_name>
    set report_format {html mht pdf rtf text}
    set runtime <count_int>
  next
end
```

Variable	Description	Default
<wvs-policy_name>	Type the name of a new or existing web vulnerability scan policy. The maximum length is 35 characters. To display the list of existing policies, type: <code>edit ?</code>	No default.
type {runonce schedule}	Select either: <ul style="list-style-type: none">runonce — Run the scan immediately after you complete the policy.schedule — Run the scan on a schedule. Also configure schedule <wvs-schedule_name>.	runonce
schedule <wvs-schedule_name>	Type the name of an existing web vulnerability scan schedule. See "config wvs schedule" on page 421 . The maximum length is 35 characters. To display the list of existing schedules, type: <code>set schedule ?</code> This setting is applicable only if <code>type</code> is <code>schedule</code> .	No default.
profile <wvs-profile_name>	Type the name of an existing web vulnerability scan profile.	No default.

Variable	Description	Default
email <email-policy_name>	Type the name of an existing email policy. See “config log email-policy” on page 72 . When the scan completes, the FortiWeb appliance will send email in the specified format to the email addresses in the policy. The maximum length is 35 characters. To display the list of existing policy, type: set email ?	No default.
report_format {html mht pdf rtf text}	Select one or more file formats of the report to attach when emailing it.	html
runtime <count_int>	Not configurable. To reset the value to zero, enter: set runtime 0	No default.

Example

The following example defines a recurring vulnerability scan with email report output in RTF and text format.

```
config wvs policy
  edit "wvs-policy1"
    set type schedule
    set schedule "wvs-schedule1"
    set report_format rtf text
    set profile "wvs-profile1"
    set email "EmailPolicy1"
  next
end
```

Related topics

- [config wvs profile](#)
- [config wvs schedule](#)

wvs profile

Use this command to display the names of web vulnerability scan profiles.



This command can only be used to display the names of the profiles. It cannot configure the profiles. To create a web vulnerability scan profile, you must use the web UI.

A web vulnerability scan (WVS) profile defines the web server to scan, as well as the specific vulnerabilities to scan for. The WVS profiles are associated with WVS policies, which determine when to perform the scan and how to publish the results of the scan defined by the profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config wvs profile
  get
  show
end
```

Example

This example displays the names of all configured web vulnerability scan profiles.

```
config wvs profile
get
```

Output:

```
== [ WVS-Profile1 ]
name: WVS-Profile1
== [ WVS-Profile2 ]
name: WVS-Profile2
```

Example

This example displays the names of all configured web vulnerability scan profiles, using configuration file syntax.

```
config wvs profile
show
```

Output:

```
config wvs profile
  edit "WVS-Profile1"
  next
  edit "WVS-Profile2"
  next
end
```

Related topics

- [config wvs policy](#)
- [config wvs schedule](#)

wvs schedule

Use this command to schedule a web vulnerability scan.

Vulnerability scanning can detect known vulnerabilities on your web servers and web applications, helping you to design protection profiles. Vulnerability scans start from an initial directory, then scan for vulnerabilities in web pages located in the same directory or subdirectory as the initial URL.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
config wvs schedule
  edit <schedule_name>
    set type {recurring | onetime}
    set date <time_str> <date_str>
    set time <time_str>
    set wday {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}
  next
end
```

Variable	Description	Default
<schedule_name>	Type the name of new or existing WVS schedule. The maximum length is 35 characters. To display the list of existing schedule, type: <code>edit ?</code>	No default.
type {recurring onetime}	Select either: <ul style="list-style-type: none"><code>onetime</code> — Run the scan only when an administrator manually initiates it. Also configure <code>date <time_str> <date_str></code>.<code>recurring</code> — Run the scan periodically, on a schedule. Also configure <code>time <time_str></code> and <code>wday {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}</code>.	onetime
date <time_str> <date_str>	For a one-time web vulnerability scan, enter the time and date for the scan to run. The time format is <code>hh:mm</code> and the date format is <code>yyyy/mm/dd</code> , where: <ul style="list-style-type: none"><code>hh</code> is the hour according to a 24-hour clock<code>mm</code> is the minute<code>yyyy</code> is the year<code>mm</code> is the month<code>dd</code> is the day Year range is 2001-2050. This only applies if <code>type</code> is <code>onetime</code> .	No default.

Variable	Description	Default
time <time_str>	Specify the time the vulnerability scan is to be performed. The time format is hh:mm, where: <ul style="list-style-type: none"> hh is the hour according to a 24-hour clock mm is the minute This only applies if type is recurring.	No default.
wday {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}	For a recurring scan only, enter one or more days of the week the scan is to be performed. This setting only applies if type is recurring.	No default.

Example

The following example schedules a recurring vulnerability scan to run every Sunday and Thursday at 1:00 AM.

```
config wvs schedule
  edit "WVS-schedule1"
    set type recurring
    set time 01:00
    set wday Sunday Thursday
  next
end
```

Related topics

- [config wvs profile](#)
- [config wvs policy](#)

diagnose

The `diagnose` commands display diagnostic information that help you troubleshoot problems. These commands do not have an equivalent in the web UI.

This chapter describes the following commands:

<code>diagnose debug</code>	<code>diagnose debug crashlog</code>	<code>diagnose network ip</code>
<code>diagnose debug application autolearn</code>	<code>diagnose debug emerglog</code>	<code>diagnose network route</code>
<code>diagnose debug application detect</code>	<code>diagnose debug flow filter</code>	<code>diagnose network rtcache</code>
<code>diagnose debug application dssl</code>	<code>diagnose debug flow reset</code>	<code>diagnose network sniffer</code>
<code>diagnose debug application fds</code>	<code>diagnose debug flow show module-process-detail</code>	<code>diagnose network tcp list</code>
<code>diagnose debug application hasync</code>	<code>diagnose debug flow trace</code>	<code>diagnose network udp list</code>
<code>diagnose debug application hatalk</code>	<code>diagnose debug info</code>	<code>diagnose policy</code>
<code>diagnose debug application http</code>	<code>diagnose debug init</code>	<code>diagnose system flash</code>
<code>diagnose debug application miglogd</code>	<code>diagnose debug reset</code>	<code>diagnose system ha mac</code>
<code>diagnose debug application mulpattern</code>	<code>diagnose debug upload</code>	<code>diagnose system ha status</code>
<code>diagnose debug application proxy</code>	<code>diagnose hardware check</code>	<code>diagnose system kill</code>
<code>diagnose debug application proxy-error</code>	<code>diagnose hardware cpu</code>	<code>diagnose system mount</code>
<code>diagnose debug application snmp</code>	<code>diagnose hardware fail-open</code>	<code>diagnose system top</code>
<code>diagnose debug application ssl</code>	<code>diagnose hardware harddisk</code>	
<code>diagnose debug application sysmon</code>	<code>diagnose hardware interrupts</code>	
<code>diagnose debug application ustack</code>	<code>diagnose hardware logdisk info</code>	
<code>diagnose debug application waf-fds-update</code>	<code>diagnose hardware mem</code>	
<code>diagnose debug cli</code>	<code>diagnose hardware nic</code>	
<code>diagnose debug cmdb</code>	<code>diagnose hardware raid list</code>	
<code>diagnose debug comlog</code>	<code>diagnose index</code>	
<code>diagnose debug console timestamp</code>	<code>diagnose log</code>	
	<code>diagnose network arp</code>	

debug

Use this command to turn debug log output on or off.



Debug logging can be very resource intensive. To minimize the performance impact on your FortiWeb appliance, use packet capture only during periods of minimal traffic, with a local console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

By default, the most verbose logging that is available from the web UI for any log type is the *Information* severity level. Due to their usually unnecessary nature, logs at the severity level of *Debug* are disabled and hidden. They can only be enabled and viewed from the CLI. Typically this is done only if your configuration seems to be correct, you cannot diagnose the problem without more information, and possibly suspect that you may have found either a hardware failure or software bug.

To generate debug logs, you must:

1. Set the verbosity level for the specific module whose debugging information you want to view, via a debug log command such as:
`debug application hasync hasync [{-1 | 0 | 1 | 2 | 4 | 8}]`
2. If necessary configure any filters specific to the module whose debugging information you are viewing, such as:
`debug flow filter server-ip 10.0.0.10`
3. If necessary start debugging specific to the module, such as:
`debug flow trace start`
4. Enable debug logs overall. To do this, enter:
`diagnose debug enable`
5. View the debug logs. For convenience, debugging logs are immediately output to your local console display or terminal emulator, but debug log files can also be uploaded to a server. For more complex issues or bugs, this may be required in order to send debug information to [Fortinet Technical Support](#). To do this, use the command:
`diagnose debug upload`



Debug logs will be generated only if the application is running. To verify this, use [diagnose system top](#). Otherwise, use [diagnose debug crashlog](#) instead.

6. The CLI will display debug logs as they occur until you either:
 - Disable it by either typing:
`diagnose debug disable`
or setting all modules' debug log verbosity back to 0. To reset all verbosity levels simultaneously, you can use the command:
`diagnose debug reset`
 - Close your terminal emulator, thereby ending your administrative session.
 - Send a termination signal to the console by pressing Ctrl+C.
 - Reboot the appliance. To do this, you can use the command:
`execute reboot`

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug {enable | disable}
```

Variable	Description	Default
debug {enable disable}	Select whether to enable or disable recording of logs at the debug severity level.	disable

Related topics

- [diagnose debug application autolearn](#)
- [diagnose debug application detect](#)
- [diagnose debug application dssl](#)
- [diagnose debug application fds](#)
- [diagnose debug application hasync](#)
- [diagnose debug application hatalk](#)
- [diagnose debug application http](#)
- [diagnose debug application miglogd](#)
- [diagnose debug application mulpattern](#)
- [diagnose debug application proxy](#)
- [diagnose debug application proxy-error](#)
- [diagnose debug application snmp](#)
- [diagnose debug application ssl](#)
- [diagnose debug application sysmon](#)
- [diagnose debug application ustack](#)
- [diagnose debug application waf-fds-update](#)
- [diagnose debug cli](#)
- [diagnose debug crashlog](#)
- [diagnose debug flow trace](#)
- [diagnose debug upload](#)
- [diagnose log](#)

debug application autolearn

Use this command to view and set the verbosity level of debug logs for auto-learning.

Before you can see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application autolearn [{autolearn_int}]
```

Variable	Description	Default
autolearn [{autolearn_int}]	<p>Specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for auto-learning and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>autolearn debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application detect

Use this command to set the verbosity level of debug logs for intrusion detection.

Before you can see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application detect [{0-7}]
```

Variable	Description	Default
detect [{0-7}]	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for intrusion detection and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level:</p> <pre>detect debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application dssl

Use this command to set the verbosity level of debug logs for SSL inspection (temporary decryption in order to enforce policies). SSL inspection is used only when FortiWeb is operating in a mode that supports it, such as transparent inspection mode or offline protection mode.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application dssl [{0-7}]
```

Variable	Description	Default
dssl [{0-7}]	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for SSL inspection and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>dssl debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application fds

Use this command to set the verbosity level of debug logs for update requests to the Fortinet Distribution Network (FDN).

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application fds [{0-7}]
```

Variable	Description	Default
<code>fds [{0-7}]</code>	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for FDN updates and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>fds debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application hasync

Use this command to set the verbosity level and type of debug logs for HA synchronization.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application hasync [{-1 | 0 | 1 | 2 | 4 | 8}]
```

Variable	Description	Default
hasync [{-1 0 1 2 4 8}]	<p>Optionally, type the number indicating the verbosity level and type of debugging messages to output to the CLI display after the command executes.</p> <ul style="list-style-type: none">-1 — Display all messages.0 — Do not display messages.1 — Display application messages such as MD5 checksums for the configuration, and confirmation that the standby appliance received the synchronized data.2 — Display network transmission messages, such as ARP broadcasts and bridge down/up status changes.4 — Display packet transmission messages.8 — Display messages about configuration file (fwb_system.conf) merges. <p>If you omit the number, the CLI displays the current verbosity level:</p> <pre>hasync debug level is 0</pre>	0

Example

This example enables diagnostic debug logging in general, then specifically enables packet transmission logging of the HA synchronization daemon, `hasyncd`.

```
diagnose debug enable
diagnose debug application hasync level 4
```

The CLI displays output such as the following until the command is terminated:

```

FortiWeb # (ha_sync.c : 624) : No element in ha send queue
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 447
(ha_send_queue.c : 242) : read send request from local, len = 450
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync.c : 454) : msglen : 23, msgbuf : config system dns
end

(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 171
(ha_sync_send.c : 383) : sent conf(0) return 171 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync.c : 454) : msglen : 26, msgbuf : config system global
end

(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 174
(ha_sync_send.c : 383) : sent conf(0) return 174 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 624) : No element in ha send queue
(ha_sync.c : 624) : No element in ha send queue
(ha_sync.c : 624) : No element in ha send queue
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 424
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 178
(ha_sync_send.c : 383) : sent conf(0) return 178 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 624) : No element in ha send queue
(ha_sync.c : 624) : No element in ha send queue
(ha_sync_recv.c : 362) : Got an valid packet, len = 180
(ha_sync_recv.c : 759) : Enter Fun : sync_recv_msg
(ha_sync_recv.c : 248) : Enter Fun : _sync_packet_check_msg, buflen =
180
(ha_sync_recv.c : 262) : msg body ssid : AC6C02
(ha_sync_recv.c : 285) : add new pkt_ss_id to last_pkt_ss_id[8]
(ha_sync_recv.c : 780) : We recvd an valid SYNC_MSG(29) packet
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 440
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 424
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync.c : 454) : msglen : 16, msgbuf : 2â€Ÿ0
(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 164
(ha_sync_send.c : 383) : sent conf(0) return 164 bytes

```

```
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 178
(ha_sync_send.c : 383) : sent conf(0) return 178 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
```

The results indicate that, initially, the MD5 configuration hash did not indicate any configuration changes (No element in ha send queue). But then an administrator changed the configuration, perhaps through the web UI, and the appliance detected changes to its DNS (msgbuf : config system dns) and global (msgbuf : config system global) settings. The active appliance then sent the changes to the standby appliance (Send conf success from [hbdev], and got reply); causes of success or failure is detailed by other debugging messages, such as the number of items in the synchronization queue (total cnt : 1, cur cnt : 0), and the number of bytes transferred from the synchronization buffer (send buf len = 178).

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application hataalk

Use this command to set the verbosity level and type of debug logs for HA heartbeats.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application hataalk [{-1 | 0 | 1 | 2}]
```

Variable	Description	Default
[{-1 0 1 2}]	<p>Optionally, type the number indicating the verbosity level and type of debugging messages to output to the CLI display after the command executes.</p> <ul style="list-style-type: none">-1 — Display all messages.0 — Do not display messages.1 — Display application messages such as MD5 checksums for the configuration, and confirmation that the standby appliance received the synchronized data.2 — Display network transmission messages, such as ARP broadcasts and bridge down/up status changes. <p>If you omit the number, the CLI displays the current verbosity level:</p> <pre>hataalk debug level is 0</pre>	0

Example

This example enables diagnostic debug logging in general, then specifically enables complete debug logging of the HA heartbeat daemon, `hataalkd`.

```
diagnose debug enable
diagnose debug application hataalk -1
```

The CLI displays output such as the following until the command is terminated:

```
FortiWeb # (ha_hb.c : 176) : mem-table[0]:
(ha_hb.c : 61) :      member name : wasp
(ha_hb.c : 62) :      member pcnt : 0
(ha_hb.c : 63) :      member pri : 5
(ha_hb.c : 64) :      member sn : FV-1KC3R11700136
(ha_hb.c : 65) :      member age : 11209
(ha_hb.c : 66) :      member role : 1
(intf_check.c : 273) : clicfg->monitor_count : 1, count : 1
(ha_hb_send.c : 85) : sock : 26, sendlen : 264(head: 88, mem(2) 88)
(ha_hb_send.c : 104) : Send HB buf success.
(ha_hb.c : 83) : Enter Function : get_master_sn
(ha_hb.c : 756) : -----
```

```

(ha_hb.c : 760) : ==> HB..., I'am (Master) master is :
FV-1KC3R11700094
(ha_hb.c : 637) : update my status info : FV-1KC3R11700094
(ha_hb.c : 871) : Enter Fun : hb_packet_check
(ha_hb.c : 897) : mysn : FV-1KC3R11700094(0), comesn :
FV-1KC3R11700136(1)
(ha_hb_recv.c : 446) : Got an valid HB packet(port3), len : 176
(ha_hb_recv.c : 451) : come from : FV-1KC3R11700136
(ha_hb_recv.c : 104) : fill ha member to local
(ha_hb_recv.c : 251) : slave (FV-1KC3R11700136) arrived ...
(ha_hb_recv.c : 342) : An exist slave device arrive...
(ha_hb_recv.c : 512) : sockfd1 : 200(UP), sockfd2 : 0(DOWN)
(ha_hb.c : 159) : Enter Function : print_member_tab
(ha_hb.c : 166) : total cnt : 2

```

(output truncated)

```

(main.c : 1005) : send short cli msg to :
FV-1KC3R11700136
(main.c : 1349) : switch MASTER -> SLAVE
(main.c : 1350) : block ARP
(main.c : 1219) : HA device into Slave mode
(main.c : 1220) : device block ARP
(main.c : 1121) : Get BrgInfo, my brgCnt = 0

```

The results indicate that the HA cluster is named `wasp` (group ID 0, HA link over port3). It is formed by the active appliance `FV-1KC3R11700094` (device priority 5) and the standby appliance `FV-1KC3R11700136`. The two appliances then switched rules — that is, a failover occurred.

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application http

Use this command to set the verbosity level of debug logs for the HTTP protocol parser. This parser module dissects the HTTP headers and content body for analysis by other modules such as rewriting, HTTP protocol constraints, server information disclosure, and attack signature matching.



If the debug logs indicate that the HTTP protocol parser may be encountering an error condition, you can temporarily disable it and allow packets to bypass it to verify if this is the case. See `noparse {enable | disable}` in “server-policy policy” on page 140.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

`diagnose debug application http [{0-7}]`

Variable	Description	Default
<code>http [{0-7}]</code>	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for the HTTP protocol parser and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>http debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)
- [diagnose debug flow trace](#)

debug application miglogd

Use this command to set the verbosity level of debug logs for the log daemon, miglogd.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application miglogd [{0-7}]
```

Variable	Description	Default
miglogd [{0-7}]	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for the log daemon and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>miglogd debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)
- [execute db rebuild](#)

debug application mulpattern

Use this command to set the verbosity level of debug logs for the pattern matching module.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application mulpattern [{0-7}]
```

Variable	Description	Default
mulpattern [{0-7}]	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for the pattern matching module and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>mulpattern debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application proxy

Use this command to set the verbosity level of debug logs for flow through the XML application proxy.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

`diagnose debug application proxy [{0-7}]`

Variable	Description	Default
proxy [{0-7}]	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for the XML application proxy flow and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>proxy debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application proxy-error

Use this command to set the verbosity level of debug logs for errors in the XML application proxy.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application proxy-error [{-1 | 0}]
```

Variable	Description	Default
proxy-error [{-1 0}]	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for XML application proxy errors and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>proxy-error debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application snmp

Use this command to debug the SNMP daemon.

Syntax

```
diagnose debug application snmp <snmp_int>
```

Variable	Description	Default
snmp <snmp_int>	<p>Specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables SNMP debugging and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level:</p> <pre>snmp debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application ssl

Use this command to set the verbosity level of debug logging for SSL/TLS offloading. SSL offloading is supported only when the FortiWeb appliance is operating in reverse proxy mode or true transparent proxy mode.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application ssl [{0-7}]
```

Variable	Description	Default
ssl [{0-7}]	<p>Specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logging of SSL/TLS offloading and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>ssl debug level is 0</pre>	0

Example

This example enables diagnostic debug logging overall, then specifically enables debug logging for SSL in reverse proxy mode.

```
diagnose debug enable
diagnose debug application ssl
```

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application sysmon

Use this command to debug the system monitor.

Syntax

```
diagnose debug application sysmon <sysmon_int>
```

Variable	Description	Default
sysmon <sysmon_int>	<p>Specifies the Sysmon debug level.</p> <p>Valid range is 0 to 7, where 0 disables system monitor debugging and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <p>sysmon debug level is 0</p>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application ustack

Use this command to set the verbosity level of debug logs for the user-space TCP/IP connectivity stack.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application ustack [{0-7}]
```

Variable	Description	Default
ustack [{0-7}]	<p>Specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logging of the user-space TCP/IP connectivity stack and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>ustack debug level is 0</pre>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug application waf-fds-update

Use this command to debug the FortiGuard service update processs.

Syntax

```
diagnose debug application waf-fds-update <fds-update_int>
```

Variable	Description	Default
waf-fds-update <fds-update_int>	<p>Specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables FortiGuard Distribution Server (FDS) update debugging and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <p>waf-fds-update debug level is 0</p>	0

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug cli

Use this command to set the debug level for the command line interface (CLI).

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug cli [{0-7}]
```

Variable	Description	Default
cli [{0-7}]	<p>Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes.</p> <p>Valid range is 0 to 7, where 0 disables debug logs for the CLI and 7 generates the most verbose logging.</p> <p>If you omit the number, the CLI displays the current verbosity level. For example:</p> <pre>cli debug level is 0</pre>	3

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug cmdb

Use this command to enable the debug log for the configuration management database (CMDB).

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account's access control profile requires only `read` permission in any profile area.

Syntax

```
diagnose debug cmdb
```

Related topics

- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug upload](#)

debug comlog

Use this command to enable or disable saving to disk of kernel or daemon core dump logs when you press the NMI button on the appliance. This button is not available on all models. For details, see the [FortiWeb NMI & COMlog Technical Note](#) and your model's QuickStart Guide.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug comlog daemon enable
diagnose debug comlog kernel enable
diagnose debug comlog daemon show
diagnose debug comlog kernel show
diagnose debug comlog daemon clear
diagnose debug comlog kernel clear
diagnose debug comlog info
```

Related topics

- [diagnose debug reset](#)
- [diagnose debug info](#)

debug console timestamp

Use this command to enable or disable the timestamp in debug logs.

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug console timestamp [{enable | disable}]
```

Variable	Description	Default
timestamp [{enable disable}]	Type enable to add timestamps to debug output or disable to remove them. If you omit the selection, the CLI displays the current timestamp status: console timestamp is disabled.	disable

Related topics

- [diagnose debug reset](#)
- [diagnose debug info](#)

debug crashlog

Use this command to show crash logs from application proxies that have call back traces, segmentation faults, or memory register dumps, or to delete the crash log.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug crashlog show
diagnose debug crashlog clear
```

Example

```
diagnose debug crashlog show
```

Output similar to the following appears in the CLI:

```
2011-02-08 06:20:46 <18632> firmware FortiWeb-1000B
4.20,build0403,110131
2011-02-08 06:20:46 <18632> application proxy
2011-02-08 06:20:46 <18632> *** signal 11 (Segmentation fault) received
***
2011-02-08 06:20:46 <18632> Register dump:
2011-02-08 06:20:46 <18632> RAX: 00000000 RBX: 00000001 RCX: 00000001
RDX: 00000001
2011-02-08 06:20:46 <18632> RSI: 008d91a4 RDI: 00000000 RBP:
2b8f90ee2b10 RSP: 0072af60
2011-02-08 06:20:46 <18632> RIP: 008d8660 EFLAGS: 2b8f9aaa0010
2011-02-08 06:20:46 <18632> CS: 86b0 FS: 0000 GS: 008d
2011-02-08 06:20:46 <18632> Trap: 7fff26859ee0 Error: 008d8710
OldMask: 00440f90
2011-02-08 06:20:46 <18632> CR2: 00010202
2011-02-08 06:20:46 <18632> Backtrace:
2011-02-08 06:20:46 <18632> [0x008d8660] => /bin/xmlproxy
(g_proxy+0x00000000)
2011-02-08 06:20:46 proxy received SEGV signal - 11
```

debug emerglog

Use this command to view or erase disk read-only error logs.

Syntax

```
diagnose debug emerglog {show | clear}
```

Variable	Description	Default
{show clear}	Type <code>show</code> to view disk read-only error logs. Type <code>clear</code> to delete error logs.	No default

debug flow filter

Use these commands to generate only packet flow debug logs that match your filter criteria, such as a specific destination IP address. You can also use these commands to delete the packet flow debug log filter, so that all packet flow debug logs are generated.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow filter clear
diagnose debug flow filter client-ip <source_ipv4>
diagnose debug flow filter direction {both | client-to-server |
server-to-client}
diagnose debug flow filter server-ip <destination_ipv4>
```

Variable	Description	Default
client-ip <source_ipv4>	Type the source (SRC) IP address of connections. This will generate only packet flow debug log messages involving that source IP address. Note: This filter operates at the IP layer, not the HTTP layer. If a load balancer or other web proxy is deployed in front of FortiWeb, and therefore all connections for HTTP requests appear to originate from this IP address, configuring this filter will have no effect. Similarly, if multiple clients share an Internet connection via NAT or explicit web proxy, configuring this filter will only isolate connections that share this IP address. It will not be able to filter out a single client based on individual HTTP sessions from that IP.	No default.
direction {both client-to-server server-to-client}	Select whether to generate only packet flow debug log messages for: <ul style="list-style-type: none">request packets (client-to-server)response packets (server-to-client)all HTTP packets (both)	both
server-ip <destination_ipv4>	Type the destination (DST) IP address of the connection, either the: <ul style="list-style-type: none">virtual server on FortiWeb (if FortiWeb is operating in reverse proxy mode)protected web server on the back end (all other operation modes) This will generate only packet flow debug log messages involving that server IP address.	No default.

Related topics

- [diagnose debug flow trace](#)

debug flow reset

Use this command to reset the configuration of packet flow debug log messages.

To use this command, your administrator account's access control profile requires only `read` permission in any profile area.

Syntax

```
diagnose debug flow reset
```

Related topics

- [diagnose debug flow filter](#)
- [diagnose debug flow show module-process-detail](#)

debug flow show module-process-detail

Use this command to include or exclude debug logs from each FortiWeb feature module (e.g. `WAF_PROTECTED_SERVER_CHECK` for the feature that tests for an allowed `Host :` name in the request) as the packet is processed when generating packet flow debug logs. This can be useful if you suspect that a module is encountering errors, or need to know which module is dropping the packet.

To use this command, your administrator account’s access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow show module-process-detail {on | off}
```

Variable	Description	Default
module-process-detail {on off}	Select whether to include (on) or exclude (off) details from each module that processes the packet.	No default.

Related topics

- [diagnose debug flow trace](#)
- [diagnose debug flow reset](#)

debug flow trace

Use this command to trace the flow of packets through the FortiWeb appliance's processing modules and network stack.

Before you will be able to see any debug logs, you must first enable debug log output using the command [diagnose debug](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow trace {start | stop}
```

Variable	Description	Default
trace {start stop}	Select whether to enable (start) or disable (stop) the recording of packet flow trace debug log messages.	No default.

Example

This example configures a filter based on the packet destination IP 172.120.20.48, enables messages from each packet processing module, enables packet flow traces, then finally begins generating the debug logs that are enabled for output (in this case, only packet trace debug logs).

Because the filters are configured **before** debug logging is enabled, the administrator can type the filter without being interrupted by debug log output to the CLI.

```
diagnose debug flow filter server-ip 172.20.120.48
diagnose debug flow show module-process-detail on
diagnose debug flow trace start
diagnose debug enable
```

Output:

```
FortiWeb # session_id=251 packet_id=0 policy_name=policy1 msg="Receive
packet from client 172.20.120.225:49428"
session_id=251 packet_id=0 msg="HTTP parsing client packet success"
session_id=251 packet_id=0 policy_name="policy1" msg="
Module name:WAF_IP_LIST_CHECK, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_X_FORWARD_FOR_PROCESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_GEO_BLOCK_LIST, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_PROTECTED_SERVER_CHECK, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_ALLOW_METHOD_PROCESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_ACTIVE_SCRIPT, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_SESSION_MANAGEMENT, Execution:4, Process error:1,
Action:ACCEPT
Module name:WAF_HTTP_DOS_PREVENTION, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_LAYER4_DOS_PREVENTION, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_AUTHENTICATION, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_GLOBAL_WHITE_LIST, Execution:4, Process error:0,
Action:ACCEPT
Module name:WAF_URL_ACCESS_POLICY, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_BRUCE_FORCE_LOGIN, Execution:3, Process error:0,
Action:ACCEPT
Module name:HTTP_CONSTRAINTS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_COOKIE_POISON, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_START_PAGES, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_PAGE_ACCESS_RULE, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_FILE_UPLOAD_RESTRICTION_POLICY, Execution:3, Process
error:0, Action:ACCEPT
Module name:ROBOT_CONTROL_PROCESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_PARAMETWER_VALIDATION_PROCESS, Execution:3, Process
error:0, Action:ACCEPT
Module name:WAF_CHUNK_DECODE, Execution:3, Process error:2,
Action:ACCEPT
Module name:WAF_FILE_UNCOMPRESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_SIG_DETECT_PROCESS, Execution:4, Process error:1,
Action:ACCEPT
```



```

Module name:WAF_HIDDEN_FIELD_PROCESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_URL_REWRITING, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_FILE_COMPRESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_CERTIFICATE_FORWARD, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_AUTOLEARN, Execution:4, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_STATISTIC, Execution:3, Process error:0,
Action:ACCEPT
"
session_id=502 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.225:49429"
session_id=502 packet_id=0 msg="HTTP parsing client packet success"
session_id=502 packet_id=0 policy_name="policy1" msg="
Module name:WAF_IP_LIST_CHECK, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_X_FORWARD_FOR_PROCESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_GEO_BLOCK_LIST, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_PROTECTED_SERVER_CHECK, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_ALLOW_METHOD_PROCESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_ACTIVE_SCRIPT, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_SESSION_MANAGEMENT, Execution:4, Process error:1,
Action:ACCEPT
Module name:WAF_HTTP_DOS_PREVENTION, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_LAYER4_DOS_PREVENTION, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_AUTHENTICATION, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_GLOBAL_WHITE_LIST, Execution:4, Process error:1,
Action:ACCEPT
Module name:WAF_URL_ACCESS_POLICY, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_BRUCE_FORCE_LOGIN, Execution:1, Process error:0,
Action:ACCEPT
Module name:HTTP_CONSTRAINTS, Execution:1, Process error:0,
Action:ACCEPT
Module name:WAF_COOKIE_POISON, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_START_PAGES, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_PAGE_ACCESS_RULE, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_FILE_UPLOAD_RESTRICTION_POLICY, Execution:3, Process
error:0, Action:ACCEPT

```

```

Module name:ROBOT_CONTROL_PROCESS, Execution:1, Process error:0,
Action:ACCEPT
Module name:WAF_PARAMETWER_VALIDATION_PROCESS, Execution:1, Process
error:0, Action:ACCEPT
Module name:WAF_CHUNK_DECODE, Execution:3, Process error:2,
Action:ACCEPT
Module name:WAF_FILE_UNCOMPRESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_SIG_DETECT_PROCESS, Execution:1, Process error:0,
Action:ACCEPT
Module name:WAF_HIDDEN_FIELD_PROCESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_URL_REWRITING, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_FILE_COMPRESS, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_CERTIFICATE_FORWARD, Execution:3, Process error:0,
Action:ACCEPT
Module name:WAF_AUTOLEARN, Execution:4, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_STATISTIC, Execution:3, Process error:0,
Action:ACCEPT
"
session_id=0 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.48:47368"
session_id=1 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.48:59682"
session_id=252 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.48:47376"
session_id=503 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.48:59687"
session_id=754 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.48:47382"
session_id=2 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.48:47385"
session_id=253 packet_id=0 policy_name=policy1 msg="Receive packet from
client 172.20.120.48:47387"
diag debug disable

```

FortiWeb #

Session lines contain the name of the matching server policy (`policy_name`), the packet identifier (`packet_ID`), and TCP session ID (`session_id`), as well as a log message (`msg`) indicating one or more of the following:

- the source IP address and port number of the packet (e.g. Receive packet from client 172.20.120.225:49428)
- the success or failure of FortiWeb's HTTP parser's attempt to analyze the HTTP headers and payload of the packet into pieces that can be scanned or modified by modules (e.g. HTTP

```
parsing client packet success or Packet dropped by detection
module, and module number=11)
```



If the debug logs indicate that the HTTP protocol parser may be encountering an error condition, you can temporarily disable it and allow packets to bypass it to verify if this is the case. See [noparse {enable | disable}](#) in “server-policy policy” on page 140.

If enabled, module lines contain messages from each FortiWeb feature module as it processes the packet (e.g. `Module name:WAF_PROTECTED_SERVER_CHECK` for the feature that tests for an allowed `Host: name` in the request). The module logs are displayed in their order of execution (for details, see the [FortiWeb Administration Guide](#)). These messages indicate:

- whether or not the module executed, and if not, the reason (e.g. `Execution:1`)
- processing errors, if any (e.g. `Process error:0`)
- whether a module has allowed or blocked the packet (e.g. `Action:ACCEPT` or `Action:FOLLOWUP_ACCEP`)

For non-execution reasons, possible status codes are:

- `Execution:1` — The module is disabled, and therefore is being skipped.
- `Execution:2` — The module is not supported in the current deployment mode, and therefore is being skipped.
- `Execution:3` — The client IP address is whitelisted, and therefore the module is being skipped.
- `Execution:4` — URL access policy has caused the module to be skipped.

Related topics

- [config server-policy policy](#)
- [config server-policy dserver](#)
- [config server-policy pserver](#)
- [config server-policy pservers](#)
- [config waf ip-list](#)
- [config waf url-access url-access-rule](#)
- [diagnose policy](#)
- [diagnose debug application http](#)
- [diagnose debug flow filter](#)
- [diagnose debug flow show module-process-detail](#)
- [diagnose debug](#)

debug info

Use this command to display a list of debug log settings.

To use this command, your administrator account's access control profile requires only `read` permission in any profile area.

Syntax

```
diagnose debug info
```

Example

```
diagnose debug application ssl 8
diagnose debug application dssl 8
diagnose debug application ustack 8
diagnose debug info
```

Output similar to the following appears in the CLI:

```
debug output:          disable
console timestamp:     disable
ssl debug level:       8
ustack debug level:    8
dssl debug level:      8
CLI debug level:       3
```

If you have not modified any verbosity levels, only this default output appears:

```
FortiWeb # diagnose debug info
debug output:          disable
console timestamp:     disable
CLI debug level:       3
```

Related topics

- [diagnose debug reset](#)
- [diagnose debug](#)
- [diagnose debug console timestamp](#)
- [diagnose debug application autolearn](#)
- [diagnose debug application detect](#)
- [diagnose debug application dssl](#)
- [diagnose debug application fds](#)
- [diagnose debug application hasync](#)
- [diagnose debug application hataalk](#)
- [diagnose debug application http](#)
- [diagnose debug application miglogd](#)
- [diagnose debug application mulpattern](#)
- [diagnose debug application proxy](#)
- [diagnose debug application proxy-error](#)
- [diagnose debug application ssl](#)
- [diagnose debug application ustack](#)
- [diagnose debug cli](#)

debug init

Syntax

diagnose debug `init` [{enable | disable}]

Variable	Description	Default
<code>init</code> [{enable disable}]	Select whether to enable (start) or disable (stop) the recording of packet flow trace debug log messages. If you omit the selection, the CLI displays the current timestamp status: <code>init output: disabled</code>	No default.

debug reset

Use this command to reset all debug log settings to default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores the factory default settings.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug reset
```

Related topics

- [diagnose debug info](#)
- [diagnose debug console timestamp](#)
- [diagnose debug application autolearn](#)
- [diagnose debug application detect](#)
- [diagnose debug application dssl](#)
- [diagnose debug application fds](#)
- [diagnose debug application hasync](#)
- [diagnose debug application hatalk](#)
- [diagnose debug application http](#)
- [diagnose debug application miglogd](#)
- [diagnose debug application mulpattern](#)
- [diagnose debug application proxy](#)
- [diagnose debug application proxy-error](#)
- [diagnose debug application ssl](#)
- [diagnose debug application ustack](#)
- [diagnose debug cli](#)

debug upload

Use this command to upload debug logs to an FTP server. This can be used if you want to view logs outside of the CLI, or if you need to provide debug log files to [Fortinet Technical Support](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug upload <ftp_ipv4> <user_str> <password_str>  
<upload-dir_str>
```

Variable	Description	Default
<ftp_ipv4>	Enter the IP address or domain name of the FTP server.	No default.
<user_str>	Enter a valid user account name to log in to the FTP server.	No default.
<password_str>	Enter the password for the user account.	No default.
<upload-dir_str>	Enter the directory path on the FTP server where FortiWeb will upload files.	No default.

Example

```
diagnose debug upload 10.1.1.5 user1 lpassw0Rd C:/uploads
```

Related topics

- [diagnose debug](#)
- [execute db rebuild](#)

hardware check

Use this command to check the appliance hardware for errors. (In the case of FortiWeb-VM, this command checks virtual hardware — the vCPUs.)

For example, to troubleshoot a logging problem, use the following command to check the log disk for errors:

```
diagnose hardware check logdisk
```

If the disk does not pass the check, it is likely the source of the problem.

Syntax

```
diagnose hardware check {all |cp8 |cpu |logdisk | memory |nic}
```

Variable	Description	Default
{all cp8 cpu logdisk memory nic}	Enter the type of hardware to check, or enter <code>all</code> to check all hardware. For FortiWeb-VM versions, the <code>cp8</code> option is not available.	No default.

Example

The following command checks the log disk:

```
diagnose hardware check logdisk
```

Output similar to the following appears in the CLI:

```
logdisk check Pass
size Pass 1952
disk-number Pass 2
raid-level Pass raid1
```

hardware cpu

Use this command to display a list of hardware specifications on the FortiWeb appliance for CPUs. (In the case of FortiWeb-VM, this command displays virtual hardware information — the vCPUs.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware cpu [list]
```

Example

```
diagnose hardware cpu list
```

Output similar to the following appears in the CLI:

```
processor           : 0
vendor_id          : GenuineIntel
cpu family         : 6
model              : 23
model name         : Intel(R) Xeon(R) CPU           E5405   @ 2.00GHz
stepping           : 10
cpu MHz            : 1995.056
cache size         : 6144 KB
physical id        : 0
siblings           : 4
core id            : 0
cpu cores          : 4
fpu                : yes
fpu_exception      : yes
cpuid level        : 13
wp                 : yes
flags               : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge
mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall
nx lm constant_tsc pni monitor ds_cpl vmx tm2 cx16 xtpr lahf_lm
bogomips           : 3994.51
clflush size       : 64
cache_alignment    : 64
address sizes      : 38 bits physical, 48 bits virtual
power management:
```

Related topics

- [diagnose system top](#)
- [diagnose hardware mem](#)
- [get system performance](#)

hardware fail-open

Fail-to-wire/bypass behavior is available for specific models only. See [“config config system fail-open” on page 205](#).

hardware harddisk

Use this command to display a list of hard disks and their capacity in megabytes (MB) in the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware harddisk [list]
```

Example

```
diagnose hardware harddisk list
```

Output similar to the following appears in the CLI:

name	size (M)
sda	625.56
sdb	32212.25

On a FortiWeb 1000C with a single properly functioning internal hard disk plus its internal flash disk, this command should show two file systems:

name	size (M)
sda	1000204.89
sdb	1971.32

where `sda`, the larger file system, is from the hard disk used to store non-configuration/firmware data. If it does not appear, you can reboot and attempt to run a file system check to fix the file system and mount it.

Similarly FortiWeb 3000D shows:

name	size (M)
sda	1999844.15
sdb	2055.21

Related topics

- [diagnose hardware logdisk info](#)
- [diagnose hardware raid list](#)
- [diagnose system flash](#)
- [diagnose system mount](#)
- [get system performance](#)

hardware interrupts

Use this command to display input/output (I/O) interrupt requests (IRQs) on the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware interrupts [list]
```

Example

```
diagnose hardware interrupts list
```

Output similar to the following appears in the CLI:

```
CPU0
 0:      225   IO-APIC-edge   timer
 1:      597   IO-APIC-edge   i8042
 2:         0    XT-PIC-XT-PIC  cascade
12:         6   IO-APIC-edge   i8042
14:         0   IO-APIC-edge   ide0
15:         0   IO-APIC-edge   ide1
16:    151462   IO-APIC-fasteoi  vmxnet ether
17:   1080446   IO-APIC-fasteoi  ioc0, vmxnet ether
18:    357613   IO-APIC-fasteoi  vmxnet ether
19:    150107   IO-APIC-fasteoi  vmxnet ether
NMI:         0   Non-maskable interrupts
LOC: 103791489   Local timer interrupts
SPU:         0   Spurious interrupts
PMI:         0   Performance monitoring interrupts
IWI:         0   IRQ work interrupts
RES:         0   Rescheduling interrupts
CAL:         0   Function call interrupts
TLB:         0   TLB shootdowns
MCE:         0   Machine check exceptions
MCP:        346   Machine check polls
ERR:         0
MIS:         0
```

Related topics

- [get system performance](#)

hardware logdisk info

Use this command to display the capacity, partitions, mount status, and RAID level (if any) of the hard disk FortiWeb uses to store logs and other data. For FortiWeb-VM, information for virtual hardware (the vDisk) is displayed.

To use this command, your administrator account's access control profile must have at least `rx` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware logdisk info
```

Example

This example shows normal output for a FortiWeb-VM installation: there is no RAID, and it has been allocated a 40 GB vDisk. If the disk were mounted as read-only, this would indicate that the disk had failed to mount normally, and would be the cause if no new log messages were being recorded.

```
diagnose hardware logdisk info
```

The CLI displays output that is similar to the following:

```
disk number: 1
disk[0] size: 31.46GB
raid level: no raid exists
partition number: 1
mount status: read-write
```

Related topics

- [diagnose hardware harddisk](#)
- [diagnose log](#)
- [diagnose system mount](#)
- [get system performance](#)

hardware mem

Use this command to display the usage statistics of ephemeral memory (RAM), including swap pages and shared memory (Shmem), on the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware — the vRAM.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware mem [list]
```

Example

```
diagnose hardware mem list
```

Output similar to the following appears in the CLI:

```
MemTotal:      1026808  kB
MemFree:       397056  kB
Buffers:       121248  kB
Cached:        86112   kB
SwapCached:    0       kB
Active:        324664  kB
Inactive:      66608   kB
Active(anon):  186544  kB
Inactive(anon): 8856   kB
Active(file):  138120  kB
Inactive(file): 57752  kB
Unevictable:   46008  kB
Mlocked:       46008  kB
SwapTotal:     0       kB
SwapFree:      0       kB
Dirty:         1564   kB
Writeback:     0       kB
AnonPages:     229920  kB
Mapped:        12632  kB
Shmem:         11488  kB
Slab:          36564  kB
SReclaimable:  6552   kB
SUnreclaim:    30012  kB
KernelStack:   640    kB
PageTables:    8820   kB
NFS_Unstable:  0       kB
Bounce:        0       kB
WritebackTmp:  0       kB
CommitLimit:   513404  kB
Committed_AS:  1216900 kB
VmallocTotal:  34359738367 kB
VmallocUsed:    38960  kB
VmallocChunk:  34359682723 kB
DirectMap4k:   8192   kB
DirectMap2M:   1040384 kB
```

Related topics

- [diagnose policy](#)
- [diagnose system flash](#)
- [diagnose system top](#)
- [get system performance](#)

hardware logdisk info

Use this command to display the capacity, partitions, mount status, and RAID level (if any) of the hard disk used to store logs and other data on the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware — the vDisk.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware logdisk info
```

Example

This example shows normal output for a FortiWeb-VM installation: there is no RAID, and it has been allocated a 40 GB vDisk. If the disk were mounted as read-only, this would indicate that the disk had failed to mount normally, and would be the cause if no new log messages were being recorded.

```
FortiWeb# diagnose hardware logdisk info
disk number: 1
disk[0] size: 31.46GB
raid level: no raid exists
partition number: 1
mount status: read-write
```

Related topics

- [diagnose hardware harddisk](#)
- [diagnose log](#)
- [diagnose system mount](#)
- [get system performance](#)

hardware nic

Use this command to display a list of hardware specifications for the network interface card (NIC) physical ports on the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware — the vNICs — and therefore the driver will be a virtual driver such as `vmxnet`, and the interrupt will be a virtual IRQ address.)

If the FortiWeb's network hardware has failed, this command can help to detect it. For example, if you know that the network cable is good and the configuration is correct, but this command displays `Link detected: no`, the physical network port may be broken.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware nic [list [<interface_name>]]
```

Variable	Description	Default
[<interface_name>]	<p>Optionally, type the name of a physical network interface, such as <code>port1</code>, to display its link status, configuration, hardware information, status, and connectivity statistics such as collision errors.</p> <p>If you omit the name of a NIC port, the CLI returns a list of all physical network interfaces, as well as the loopback interface (<code>lo</code>):</p> <pre>lo port1 port2 port3 port4</pre> <p>Note: The detected physical link status from this command is <i>not</i> the same as its configured administrative status.</p> <p>For example, even though you have used config system interface to configure <code>port1</code> with <code>set status down</code>, if the cable is physically plugged in, <code>diagnose hardware nic list port1</code> will indicate correctly that the link is up (<code>Link detected: yes</code>).</p>	No default.

Example

```
diagnose hardware nic list
```

Output similar to the following appears in the CLI:

driver	vmxnet
version	2.0.9.0
firmware-version	N/A
bus-info	0000:00:11.0
Supported ports	TP
Supported link modes	1000baseT/Full
Supports auto-negotiation:	No
Advertised link modes:	Not reported
Advertised auto-negotiation:	No
Speed:	1000Mb/s
Duplex:	Full
Port:	Twisted Pair
PHYAD	0
Transceiver:	internal
Auto-negotiation	off
Link detected	yes
Link encap	Ethernet
HWaddr	00:0C:29:FE:2B:47
INET addr	10.1.1.221
Bcast	10.1.1.221
Mask	255.255.255.255
FLAG	UP BROADCAST RUNNING MULTICAST
MTU	1500
MEtric	1
Outfill	0
Keepalive	6846704
Interrupt	18
Base address	0x1400
RX packets	171487
RX errors	167784
RX dropped	0
RX overruns	0
RX frame	0
TX packets	202724
TX errors	0
TX dropped	0
TX overruns	0
TX carrier	0
TX collisions	0
TX queuelen	1000
RX bytes	72772373 (69.4 Mb)
TX bytes	32288070 (30.7 Mb)

Related topics

- [config system interface](#)
- [diagnose debug application ustack](#)
- [diagnose hardware interrupts](#)
- [diagnose network ip](#)
- [diagnose network sniffer](#)
- [diagnose network tcp list](#)
- [diagnose network udp list](#)
- [diagnose system ha mac](#)
- [execute traceroute](#)
- [get system performance](#)

hardware raid list

Use this command to run a diagnostic test of each hard disk in the RAID array that FortiWeb has. It also displays the capacity and RAID level. (Because FortiWeb-VM has no RAID, this command is not applicable to it.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose hardware raid list
```

Example

```
diagnose hardware raid list
```

Output similar to the following (from a FortiWeb 3000D) appears in the CLI window:

```
disk-number          size(M)  level
0 (OK) , 1 (OK) ,    1877274  raid1
```

Related topics

- [config system raid](#)
- [diagnose hardware harddisk](#)
- [diagnose system mount](#)
- [execute create-raid level](#)
- [execute create-raid rebuild](#)
- [get system performance](#)

index

Use this command to view (`list`) or clear logs, or to examine (`show`) or configure logs.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose index all show
diagnose index all clear
diagnose index {alog | dlog | elog | tlog} clear
diagnose index {alog | dlog | elog | tlog} list <index_int>
diagnose index {alog | dlog | elog | tlog} set <queue_int>
diagnose index {alog | dlog | elog | tlog} show
```

Variable	Description	Default
index {alog dlog elog tlog}	Select which log files to view or affect: <ul style="list-style-type: none">alog — Attack logs.dlog — Debug logs.elog — Event logs.tlog — Traffic logs.	No default.
list <index_int>	Type the number of most recent logs to display.	No default.
set <queue_int>	Type the maximum length of the log before it is flushed and written to disk. The valid range is from 0 to 32768.	No default.

Example

This example displays a list of logs processed.

```
diagnose index all show
```

Related topics

- [config log attack-log](#)
- [config log event-log](#)
- [config log traffic-log](#)
- [diagnose debug](#)
- [diagnose hardware logdisk info](#)

log

Use this command to view (`list`) or clear log messages, or to examine (`show`) or configure logging queues.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `loggrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose log all show
ddiagnose log {alog | dlog | elog | tlog} show
```

Variable	Description	Default
log {alog dlog elog tlog}	Select which log files to view: <ul style="list-style-type: none">alog — Attack logs.dlog — Debug logs.elog — Event logs.tlog — Traffic logs.	No default.

Example

This example displays a list of log messages.

```
diagnose log all show
```

Related topics

- [config log attack-log](#)
- [config log event-log](#)
- [config log traffic-log](#)
- [diagnose debug](#)
- [diagnose hardware logdisk info](#)

network arp

Use this command to add or delete an address resolution protocol (ARP) table entry, or to display the ARP table. The ARP table is used to resolve the IP addresses that correspond to a network interface card's physical MAC address, thereby determining which IP addresses can be reached directly through a link.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose network arp add <interface_name> {<interface_ipv4> |  
interface_ipv6>} <mac-address_hex>  
diagnose network arp delete <interface_name> {<interface_ipv4> |  
interface_ipv6>} <mac-address_hex>  
diagnose network arp list
```

Variable	Description	Default
<interface_name>	Type the name of the interface to add or delete from the ARP table.	No default.
{<interface_ipv4> interface_ipv6>}	Type the IP address of the interface.	No default.
<mac-address_hex>	Type the MAC address of the interface.	No default.

Example

This example displays a list of ARP table entries and then deletes one.

```
diagnose network arp list  
IP address      HW type      Flags      HW address      Mask  
Device  
172.20.120.29   0x1          0x2        00:13:72:38:72:21 *  
port1  
172.20.120.26   0x1          0x2        00:26:2D:24:B7:D3 *  
port2  
diagnose network arp delete port2 172.20.120.26 00:26:2D:24:B7:D3
```

Related topics

- [diagnose network route](#)
- [diagnose network ip](#)
- [config router static](#)
- [config system interface](#)

network ip

Use these commands to add or delete a network interface, loopback interface, or virtual server (which functions somewhat like a virtual network interface) IP address, or to list the table of network interface IPs.



Back up the configuration before deleting a network interface table entry (see [“execute backup full-config” on page 510](#)). FortiWeb presents no confirmation message, and in some cases such as the loopback interface, provides no undelete mechanism.

To use this command, your administrator account’s access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose network ip add <interface_name> {<interface_ipv4> |  
interface_ipv6} {<interface_ipv4mask> |<interface_v6mask>}  
diagnose network ip delete <interface_name> {<interface_ipv4> |  
interface_ipv6}  
diagnose network ip list
```

Variable	Description	Default
<interface_name>	Type the name of the interface to add or delete from the network interface table.	No default.
{<interface_ipv4> interface_ipv6}	Type the IP address of the network interface.	No default.
{<interface_ipv4mask> <interface_v6mask>}	Type the subnet mask.	No default.

Example

This example displays a list of enabled network interfaces, including the loopback (lo)

```
diagnose network ip list
```

Output:

```
1 IP 127.0.0.1/255.255.255.0 lo  
2 IP 172.20.120.47/255.255.255.0 port1  
2 IP 10.1.1.221/255.255.255.255 port1  
4 IP 192.168.1.27/255.255.255.0 port3
```

Example

This example deletes the IP of a virtual server on port2.

```
diagnose network ip delete port1 10.1.1.221
```

Related topics

- [diagnose network route](#)
- [diagnose network arp](#)
- [config system interface](#)

network route

Use this command to add or delete a route in the routing table, or to list the routing table.

Unlike [get router all](#), this command displays **all** individual entries, including automatically configured routes for the loopback interface (127.0.0.1) and VLANs, and also displays each route's priority. Unlike [diagnose network rtcache](#), it displays all known routes, regardless of whether they have been recently used.



Do not delete routes unless you are sure. FortiWeb does not ask you to confirm the deletion, and there is no undelete mechanism. For example, if you accidentally delete a loopback interface route, you must recreate it manually.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose network route add {<source_ipv4mask> | <source_ipv6mask>}  
<interface_name> {<destination_ipv4mask> | <destination_ipv6mask>}  
<interface_name> {<gateway_ipv4> | <gateway_ipv6>}<priority_int>  
diagnose network route delete {<source_ipv4mask> | <source_ipv6mask>}  
<interface_name> {<destination_ipv4mask> | <destination_ipv6mask>}  
<interface_name> {<gateway_ipv4> | <gateway_ipv6>} <priority_int>
```

Variable	Description	Default
{<source_ipv4mask> <source_ipv6mask>}	Type the IP address and network mask of the source, separated by a space.	No default.
<interface_name>	Type the name of the interface to add or delete from the routing table.	No default.
{<destination_ipv4mask> <destination_ipv6mask>}	Type the IP address and network mask of the source, separated by a space.	No default.
{<gateway_ipv4> <gateway_ipv6>}	Enter the IP address of the next hop router (sometimes called a gateway) to which this route sends packets.	No default.
<priority_int>	Enter the priority of the route in the routing table. The lower the number the higher the priority. The value can be an integer from 1 to 255.	0

Example

This example displays the routing table.

```
tab=255 0.0.0.0/0.0.0.0/0->192.168.1.0/32/4 gwy=0.0.0.0 prio=0
prefsrc=192.168.1.27 type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->172.20.120.0/32/2 gwy=0.0.0.0 prio=0
prefsrc=172.20.120.47 type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->10.1.1.221/32/2 gwy=0.0.0.0 prio=0
prefsrc=10.1.1.221 type=2 scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->10.1.1.221/32/2 gwy=0.0.0.0 prio=0
prefsrc=10.1.1.221 type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.255/32/1 gwy=0.0.0.0 prio=0
prefsrc=127.0.0.1 type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->192.168.1.255/32/4 gwy=0.0.0.0 prio=0
prefsrc=192.168.1.27 type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->192.168.1.27/32/4 gwy=0.0.0.0 prio=0
prefsrc=192.168.1.27 type=2 scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->172.20.120.255/32/2 gwy=0.0.0.0 prio=0
prefsrc=172.20.120.47 type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->172.20.120.47/32/2 gwy=0.0.0.0 prio=0
prefsrc=172.20.120.47 type=2 scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.0/32/1 gwy=0.0.0.0 prio=0
prefsrc=127.0.0.1 type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.1/32/1 gwy=0.0.0.0 prio=0
prefsrc=127.0.0.1 type=2 scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.0/24/1 gwy=0.0.0.0 prio=0
prefsrc=127.0.0.1 type=2 scope=fe proto=2
tab=254 0.0.0.0/0.0.0.0/0->192.168.1.0/24/4 gwy=0.0.0.0 prio=0
prefsrc=192.168.1.27 type=1 scope=fd proto=2
tab=254 0.0.0.0/0.0.0.0/0->172.20.120.0/24/2 gwy=0.0.0.0 prio=0
prefsrc=172.20.120.47 type=1 scope=fd proto=2
tab=254 0.0.0.0/0.0.0.0/0->0.0.0.0/0/2 gwy=172.20.120.2 prio=2
prefsrc=0.0.0.0 type=1 scope=00 proto=14
```

Example

This example adds a route to the routing table.

```
diagnose network route add 10::/64 port1 10:200::1/64 port1 10::1 0
```

Related topics

- [get router all](#)
- [execute ping](#)
- [execute ping6](#)
- [execute traceroute](#)
- [diagnose network rtcache](#)
- [config router static](#)

network rtcache

Use this command to display the routing cache.

Unlike [diagnose network route](#), this command displays the cache of the most recently used routes, **not** necessarily the entire configuration. (You may have configured many routes, and these configurations will be saved to disk and appear in [diagnose network route](#), but rarely used ones will **not** usually appear in the route cache, which keeps recently used routes in RAM for performance reasons.)

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
diagnose network rtcache list
```

Example

This example displays the ARP cache.

```
172.20.120.52(port1)->255.255.255.255(lo) via 0.0.0.0, pri 0 prot 0
scope 0, ref 0 lastuse 3181 expires 0 error 0 used 855
172.20.120.100(port3)->172.20.120.255(lo) via 0.0.0.0, pri 0 prot 0
scope 0, ref 0 lastuse 434 expires 0 error 0 used 0
172.20.120.230(port1)->255.255.255.255(lo) via 0.0.0.0, pri 0 prot 0
scope 0, ref 0 lastuse 47386 expires 0 error 0 used 7
10.0.1.1(none)->10.0.1.1(lo) via 0.0.0.0, pri 0 prot 0 scope 0, ref 0
lastuse 223 expires 0 error 0 used 29551
0.0.0.0(none)->10.0.1.1(lo) via 0.0.0.0, pri 0 prot 0 scope 0, ref 0
lastuse 223 expires 0 error 0 used 7387
::(none)->::1(lo) via ::, pri 0 prot 0 scope 0 ref 1 lastuse 155845
expires 0 error 0 used 417
::(none)->2607:f0b0:f:420:20c:29ff:fe4d:3ad3(lo) via ::, pri 0 prot 0
scope 0 ref 1 lastuse 354923 expires 0 error 0 used 1
::(none)->2607:f0b0:f:420:20c:29ff:fe4d:3ae7(lo) via ::, pri 0 prot 0
scope 0 ref 1 lastuse 2590615 expires 0 error 0 used 0
::(none)->2607:f0b0:f:420:20c:29ff:fe4d:3af1(lo) via ::, pri 0 prot 0
scope 0 ref 1 lastuse 2590615 expires 0 error 0 used 0
::(none)->2607:f0b0:f:420::(port1) via ::, pri 256 prot 0 scope 0 ref 0
lastuse 2590616 expires 214715722 error 0 used 0
::(none)->ff00::(port4) via ::, pri 256 prot 0 scope 0 ref 0 lastuse
2590615 expires 0 error 0 used 0
::(none)->ff00::(lo) via ::, pri -1 prot 0 scope 0 ref 1 lastuse
449431651 expires 0 error -101 used 1
```

Example

This example adds a route to the routing table.

```
diagnose network route add vlan2 160.1.12.0 255.0.0.0 172.20.01.169 32
3 verify
```

Related topics

- [get router all](#)
- [execute ping](#)
- [execute ping6](#)
- [execute traceroute](#)
- [diagnose network route](#)
- [config router static](#)

network sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing or packet analysis, records some or all of the packets seen by a network interface (that is, the network interface is used in promiscuous mode). By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiWeb appliances have a built-in sniffer. Packet capture on FortiWeb appliances is similar to that of FortiGate appliances. Packet capture output appears on your CLI display until you stop it by pressing Ctrl+C, or until it reaches the number of packets that you have specified to capture.



Packet capture can be very resource intensive. To minimize the performance impact on your FortiWeb appliance, use packet capture only during periods of minimal traffic, with a local console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose network sniffer [{any | <interface_name>} [{none | '<filter_str>'} [{1 | 2 | 3} [<packets_int>]]]
```

Variable	Description	Default
{any <interface_name>}	Type the name of a network interface whose packets you want to capture, such as port1, or type any to capture packets on all network interfaces. If you omit this and the following parameters for the command, the command captures all packets on all network interfaces.	No default.
{none '<filter_str>'}	Type either none to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 25'. Surround the filter string in quotes (''). Filters use tcpdump syntax: '[[src dst] host {<host1_fqdn> <host1_ipv4>}] [and or] [[src dst] host {<host2_fqdn> <host2_ipv4>}] [and or] [[arp ip gre esp udp tcp] port <port1_int>] [and or] [[arp ip gre esp udp tcp] port <port2_int>] ' To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or reply packets, indicate which host is the source, and which is the destination. For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter: 'udp and port 1812 and src host 1.example.com and dst \ (2.example.com or 2.example.com \) '	none

Variable	Description	Default
{1 2 3}	<p>Type one of the following integers indicating the depth of packet headers and payloads to capture:</p> <ul style="list-style-type: none"> 1 — Display the packet capture timestamp, plus basic fields of the IP header: the source IP address, the destination IP address, protocol name, and destination port number. <p>Does not display all fields of the IP header; it omits:</p> <ul style="list-style-type: none"> IP version number bits Internet header length (ihl) type of service/differentiated services code point (tos) explicit congestion notification total packet or fragment length packet ID IP header checksum time to live (TTL) IP flag fragment offset options bits 2 — All of the output from 1, plus the packet payload in both hexadecimal and ASCII. 3 — All of the output from 2, plus the the link layer (Ethernet) header. <p>For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).</p>	1
<packets_int>	<p>Type the number of packets to capture before stopping.</p> <p>If you do not specify a number, the command will continue to capture packets until you press Ctrl+C.</p>	Packet capture continues until you press Ctrl + C.

Example

The following example captures three packets of traffic from any port number or protocol and between any source and destination (a filter of `none`), which passes through the network interface named `port1`. The capture uses a low level of verbosity (indicated by 1).

Commands that you would type are highlighted in bold; responses from the FortiWeb appliance are not bolded.

```
FortiWeb# diagnose network sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack
2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack
2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by 1). Because the filter does not specify either host as the source or destination in the IP header (`src` or `dst`), the sniffer captures both forward and reply traffic.

Commands that you would type are highlighted in bold; responses from the FortiWeb appliance are not bolded.

```
FortiWeb# diagnose network sniffer packet port1 'host 192.168.0.2 or  
host 192.168.0.1 and tcp port 80' 1
```

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl+C. The sniffer then confirms that five packets were seen by that network interface. Below is a sample output.

```
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example

The following example captures TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by 3).

The number of packets to capture is not specified, so the packet capture continues until the administrator presses Ctrl+C. The sniffer then states how many packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the FortiWeb appliance are not bolded.

```
FortiWeb# diagnose network sniffer packet port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000  0009 0f09 0001 0009 0f89 2914 0800 4500      .....E.
0x0010  003c 73d1 4000 4006 3bc6 d157 fede ac16      .<s.@.@.;..W....
0x0020  0ed8 c442 01bb 2d66 d8d2 0000 0000 a002      ...B..-f.....
0x0030  16d0 4f72 0000 0204 05b4 0402 080a 03ab      ..Or.....
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is often, but not always, preferable to analyze the output by loading it into a network protocol analyzer application such as Wireshark (<http://www.wireshark.org/>).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output to a file. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as [PuTTY](#)
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software such as [Wireshark](#)

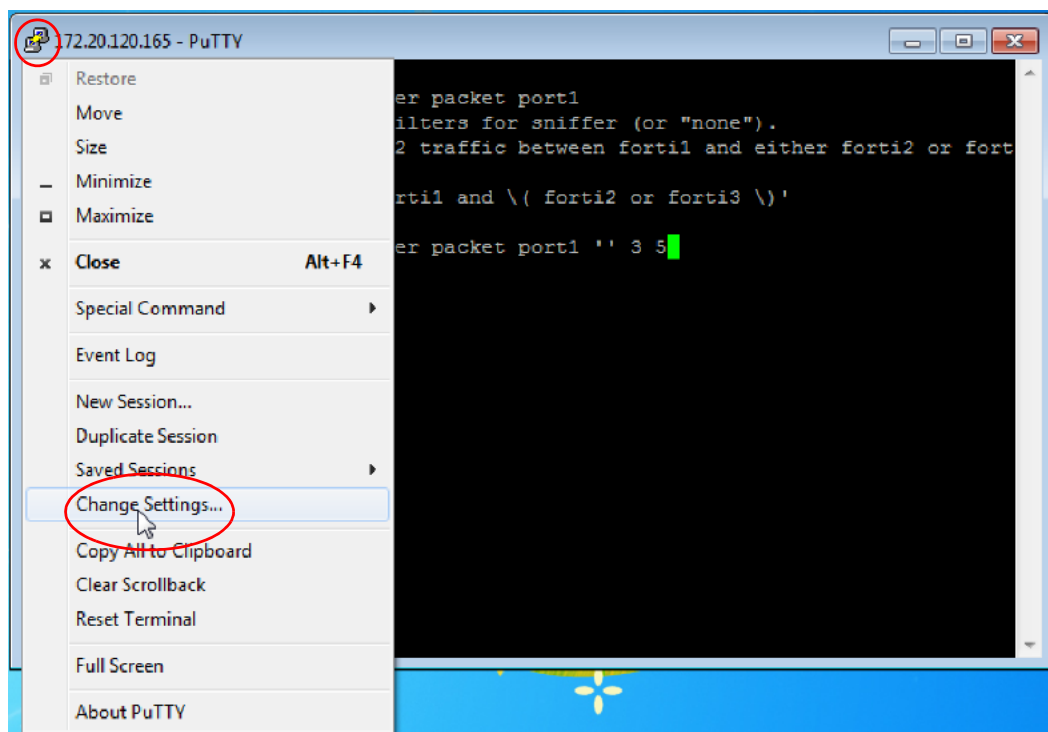
To view packet capture output using PuTTY and Wireshark

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the FortiWeb appliance using either a local console, SSH, or Telnet connection. For details, see [“Connecting to the CLI” on page 34](#).
3. Type the packet capture command, such as:

```
diag network sniffer packet port1 'tcp port 443' 3 100
```

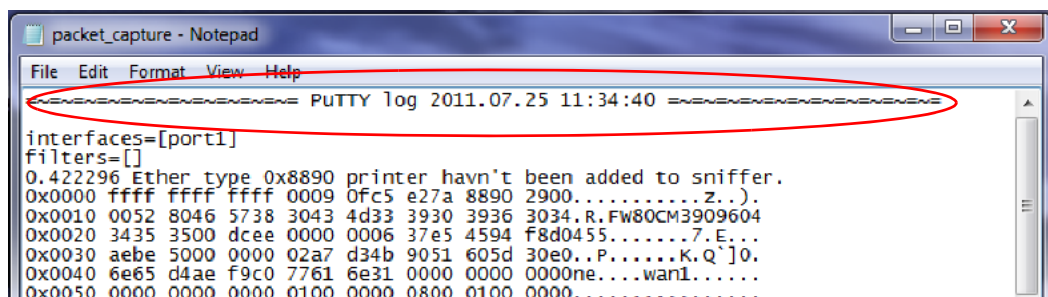
but do **not** press Enter. yet

4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.



A dialog appears where you can configure PuTTY to save output to a plain text file.

5. In the *Category* tree on the left, go to *Session > Logging*.
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)
8. Click *Apply*.
9. Press Enter to send the CLI command to the FortiMail appliance, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press `Ctrl + C` to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.



13. Delete the first and last lines, which look like this:

```
=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2014.07.25 11:34:40
~=~=~=~=~=~=~=~=~=~=~=
FortiWeb-2000 #
```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.

14. Convert the plain text file to a format recognizable by your network protocol analyzer application.

You can convert the plain text file to a format (.pcap) recognizable by Wireshark (formerly called Ethernet) using the fgt2eth.pl Perl script. To download fgt2eth.pl, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).



The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

To use fgt2eth.pl, open a command prompt, then enter a command such as the following:



Methods to open a command prompt vary by operating system.

On Windows XP, go to *Start > Run* and enter `cmd`.

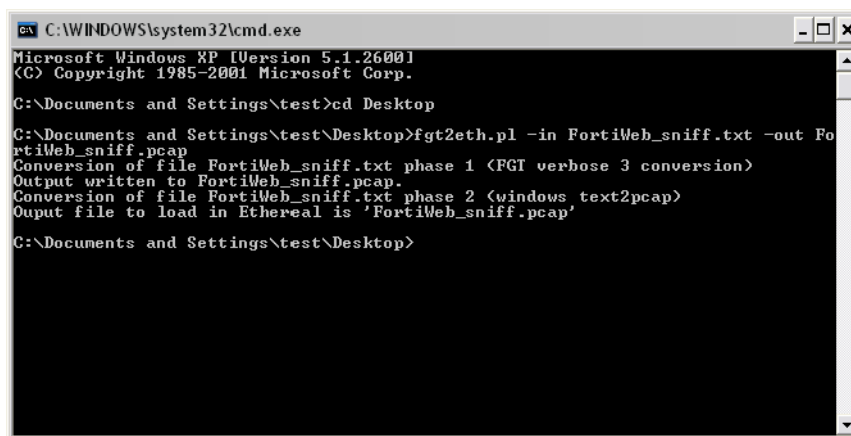
On Windows 7, click the Start (Windows logo) menu to open it, then enter `cmd`.

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved

Figure 4: Converting sniffer output to .pcap format



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

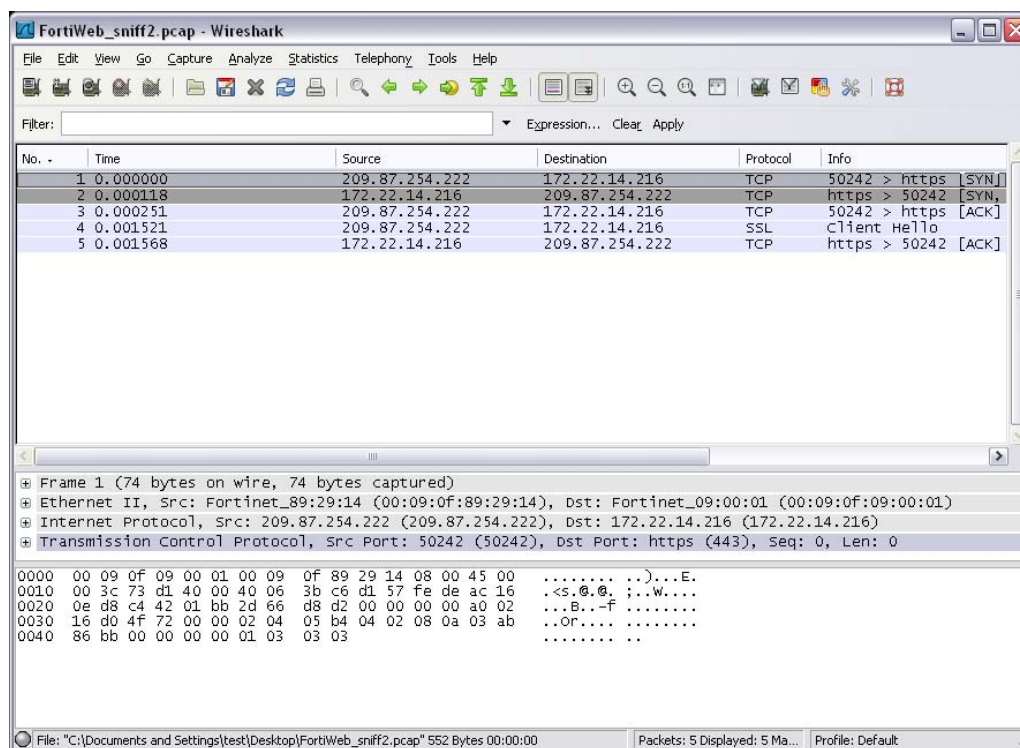
C:\Documents and Settings\test>cd Desktop

C:\Documents and Settings\test\Desktop>fgt2eth.pl -in FortiWeb_sniff.txt -out FortiWeb_sniff.pcap
Conversion of file FortiWeb_sniff.txt phase 1 (PGI verbose 3 conversion)
Output written to FortiWeb_sniff.pcap.
Conversion of file FortiWeb_sniff.txt phase 2 (windows text2pcap)
Output file to load in Ethereal is 'FortiWeb_sniff.pcap'

C:\Documents and Settings\test\Desktop>
```

15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

Figure 5: Viewing sniffer output in Wireshark



For additional information on packet capture, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).

network tcp list

Use this command to view a list of TCP raw socket details, including:

- `sl` — Kernel socket hash slot.
- `local_address` — IP address and port number pair of the local FortiWeb network interface in hexadecimal, such as `DD01010A:0050`.
- `rem_address` — Remote host's network interface and port number pair. If not connected, this will contain `00000000:0000`.
- `st` — TCP state code (e.g. `0A` for listening, `01` for established, or `06` for timeout wait)
- `tx_queue` — Kernel memory usage by the transmission queue.
- `rx_queue` — Kernel memory usage by the retransmission queues.
- `tr, tm-> when, retrnsmt` — Kernel socket state debugging information.
- `uid` — User ID of the socket's creator (on FortiWeb, always `0`).
- `timeout` — Connection timeout.
- `inode` — Pseudo-file system i-node of the process.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose network tcp list
```

Example

```
diagnose network tcp list
sl  local_address rem_address  st tx_queue rx_queue tr tm->when
retrnsmt uid timeout inode
  0: DD01010A:0050 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 333597 1 ffff88003b825880 299 0 0 2 -1
  1: 2F7814AC:0050 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 228018 1 ffff88003b824680 299 0 0 2 -1
  2: 1B01A8C0:0050 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2692 1 ffff88003b6ec6c0 299 0 0 2 -1
  3: 0100007F:0050 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2691 1 ffff88003b6eccc0 299 0 0 2 -1
  4: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2433 1 ffff88003b489280 299 0 0 2 -1
  5: 00000000:0017 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2400 1 ffff88003b489880 299 0 0 2 -1
  6: 0100007F:22B8 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2687 1 ffff88003b488680 299 0 0 2 -1
  7: DD01010A:01BB 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 333598 1 ffff88003bbf3940 299 0 0 2 -1
  8: 2F7814AC:01BB 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 228017 1 ffff88003b824080 299 0 0 2 -1
  9: 1B01A8C0:01BB 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2689 1 ffff88003b6ed8c0 299 0 0 2 -1
 10: 0100007F:01BB 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2688 1 ffff88003b488080 299 0 0 2 -1
 11: 00000000:208D 00000000:0000 0A 00000000:00000000 00:00000000
00000000 0 0 2441 1 ffff88003b488c80 299 0 0 2 -1
 12: 2F7814AC:0016 E17814AC:FEF2 01 00000000:00000000 02:000909FE
00000000 0 0 272209 4 ffff88003bbf2d40 20 3 1 5 -1
```

Related topics

- [diagnose network arp](#)
- [diagnose network ip](#)
- [diagnose debug application ustack](#)

network udp list

Use this command to view a list of UDP raw socket details, including:

- `sl` — Kernel socket hash slot.
- `local_address` — IP address and port number pair of the local FortiWeb network interface in hexadecimal, such as `DD01010A:0050`.
- `rem_address` — Remote host's network interface and port number pair. If not connected, this will contain `00000000:0000`.
- `st` — TCP state code in hexadecimal (e.g. `0A` for listening, `01` for connection established, or `06` for waiting for data)
- `tx_queue` — Kernel memory usage by the transmission (Tx) queue.
- `rx_queue` — Kernel memory usage by the retransmission (Rx) queues. (This is not used by UDP, since the protocol itself does not support retransmission.)
- `tr,tm-> when, retrnsmt` — Kernel socket state debugging information. (These are not used by UDP, since the protocol itself does not support retransmission.)
- `uid` — User ID of the socket's creator (on FortiWeb, always `0`).
- `timeout` — Connection timeout.
- `inode` — Pseudo-file system inode of the process.
- `ref, pointer` — Pseudo-file system references.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose network udp list
```

Example

```
diagnose network udp list
sl local_address rem_address st tx_queue rx_queue tr tm->when
retrnsmt uid timeout inode ref pointer drops
 307: 00000000:00A1 00000000:0000 07 00000000:00000000 00:00000000
00000000 0 0 2498 2 ffff88003acba080 0
 447: 00000000:3F2D 00000000:0000 07 00000000:00000000 00:00000000
00000000 0 0 2874 2 ffff88003acbac80 0
```

Related topics

- [diagnose network arp](#)
- [diagnose network ip](#)
- [diagnose debug application ustack](#)

policy

Use this command to view the process ID, memory usage, live sessions, and traffic statistics associated with a server policy.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose policy dashboard {all | list <policy_name>}
diagnose policy memory {all | list <policy_name>}
diagnose policy pserver list <policy_name>
diagnose policy session {list <policy_name>}
diagnose policy traffic {list <policy_name>}
diagnose policy traffic {list <policy_name>}
diagnose policy period-blockip {list <policy_name>}
diagnose policy period-blockip {delete <policy_name>}{ipv4 | ipv6}
```

Variable	Description	Default
dashboard {all list <policy_name>}	Presents information similar to that displayed on the web UI's dashboard.	No default.
memory {all list <policy_name>}	For each live session, displays the source IP and port, and the destination IP and port.	No default.
pserver list <policy_name>	Displays the status of physical servers covered by the policy.	No default.
session {list <policy_name>}	Displays IP session information for TCP and UDP connections.	No default.
traffic {list <policy_name>}	Displays traffic throughput (bandwidth usage) information.	No default.
period-blockip {list <policy_name>}	Displays client IP addresses whose requests are temporarily blocked because the client violated a rule in the specified policy with an <i>Action</i> value of <i>Period Block</i> .	No default.
period-blockip {delete <policy_name>}{ipv4 ipv6}	Unblocks the specified client IP address that FortiWeb has blocked because it violated a rule in the specified policy with an <i>Action</i> value of <i>Period Block</i> . (FortiWeb can still block the address because it violates a rule in a different policy.)	No default.
<policy_name>	Type the name of an existing server policy.	No default.

Example

This example shows the output of the `dashboard` command. The operation mode (`opmode`) is indicated by its code number:

Table 9: Operation mode (`opmode`) values

Integer	Meaning
2	True transparent proxy
4	Reverse proxy
8	Offline protection
32	Transparent inspection

```
diagnose policy dashboard list Policy1
opmode is 4
-----policy-----
name: Policy1
pid: 433
vip: 172.20.120.28
http-port: 80
https-port: 0
freemem: 21357088
-----end-----
```

Related topics

- [config server-policy policy](#)
- [diagnose network ip](#)
- [diagnose debug flow filter](#)
- [get system performance](#)

system flash

Use this command to change the currently active firmware partition or to display partition information stored on the flash drive.

FortiWeb appliances have 2 partitions that each contain a firmware image: one is the primary and one is the backup. If the FortiWeb appliance is unable to successfully boot using the primary firmware partition, it may boot using the alternative firmware partition. The second partition can contain another version of the firmware.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose system flash default <partition_int>
diagnose system flash list
```

Variable	Description	Default
<partition_int>	Type the number of the partition that will be used as the primary firmware partition during the <i>next</i> reboot or startup. The other partition will become the backup firmware partition.	No default.

Example

This example lists the partition settings.

```
diagnose system flash list
```

Below is a sample output.

Image#	Version	TotalSize (KB)	Used (KB)	Use%
Active				
1	FV-1KB-4.30-FW-build0521-110120	38733	33125	86%
No				
2	FV-1KB-4.30-FW-build0522-110112	38733	33125	86%
Yes				
3		836612	16980	2 % No

Related topics

- [execute restore image](#)
- [get system status](#)

system ha mac

Use this command to display the virtual MAC addresses and link statuses of each network interface of appliances in the HA group.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose system ha mac
```

Example

This example indicates that the links are “up” (`linkfail=0`) for port1 and port3 on the currently active appliance in the HA pair. While operating in HA, the network interfaces are using a Layer 1 data link (MAC) address that begins with the hexadecimal string `00:09:0F:09:00:.`

```
diagnose system ha mac
```

Below is a sample output.

```
HA mac msg
name=port1, phyindex=0, 00:09:0F:09:00:01, linkfail=0
name=port2, phyindex=1, 00:09:0F:09:00:02, linkfail=1
name=port3, phyindex=2, 00:09:0F:09:00:03, linkfail=0
name=port4, phyindex=3, 00:09:0F:09:00:04, linkfail=1
```

Related topics

- [execute ha disconnect](#)
- [execute ha manage](#)
- [diagnose system ha status](#)
- [get system status](#)
- [config system ha](#)

system ha status

Use this command to display the HA group ID, as well as the serial number, role (active or standby), and device priority of each appliance belonging to the HA cluster.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose system ha status
```

Example

This example lists the HA group ID, serial numbers, and device priorities.

```
diagnose system ha status
```

Below is a sample output.

HA information

```
Model=FortiWeb-1000C, Mode=a-p Group=0 Debug=0
```

```
HA group member information: is_manage_master=1.
```

```
FV-1KC3R11700094, Master:1
```

```
FV-1KC3R11700136, Slave:5
```

Related topics

- [execute ha disconnect](#)
- [execute ha manage](#)
- [diagnose system ha status](#)
- [get system status](#)
- [config system global](#)

system kill

Use this command to terminate a process currently running on FortiWeb, or send another signal from the FortiWeb OS to the process.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose system kill <signal_int> <pid_int>
```

Variable	Description	Default
<signal_int>	Type the ID of the signal to send to the process. This is an integer between 1 and 32. Some common signals are: <ul style="list-style-type: none">• 1 — Varies by the process's interpretation, such as re-read configuration files or re-initialize (hang up; <code>SIGHUP</code>). For example, the FortiWeb web UI verifies its configuration files, then restarts gracefully. <ul style="list-style-type: none">• 2 — Request termination by simulating the pressing of the interrupt keys, such as Ctrl + C (interrupt; <code>SIGINT</code>).• 3 — Force termination immediately and do a core dump (quit; <code>SIGQUIT</code>).• 9 — Force termination immediately (kill; <code>SIGKILL</code>).• 15 — Request termination by inter-process communication (terminate; <code>SIGTERM</code>).	No default.
<pid_int>	Type the process ID where the signal is sent to. To list all current process IDs, use diagnose system top .	No default.

Related topics

- [diagnose system top](#)
- [diagnose hardware cpu](#)
- [diagnose hardware mem](#)
- [get system performance](#)

system mount

Use this command to display a list of mounted file systems, including their available disk space, disk usage, and mount locations.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose system mount list
```

Example

```
diagnose system mount list
```

Output from a FortiWeb 3000D:

Filesystem	1M-blocks	Used	Available	Use%	Mounted on
/dev/ram0	97	87	10	89%	/
none	4823	0	4823	0%	/tmp
none	16077	0	16077	0%	/dev/shm
/dev/sdb1	189	45	134	25%	/data
/dev/sdb3	961	17	895	1%	/home
/dev/sda1	1877275	271	1781644	0%	/var/log

Related topics

- [diagnose hardware logdisk info](#)
- [diagnose hardware raid list](#)

system top

Use this command to view a list of the most system-intensive processes and to change the refresh rate.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
diagnose system top [<delay_int> [<max-lines>]]
```

Variable	Description	Default
<delay_int>	Type the process list refresh interval in seconds.	5
<max-lines>	Set the maximum number of top processes to display.	All processes are shown.

Once you execute this command, it continues to run and display in the CLI window until you enter `q` (quit).

While the command is running, you can press `Shift + P` to sort the five columns of data by CPU usage (the default) or `Shift + M` to sort by memory usage.

Example

This example displays a list of the top FortiWeb processes and sets the update interval at 10 seconds.

```
diagnose system top 10
```

Below is a sample output.

Run Time: 0 days, 0 hours and 48 minutes

0U, 0S, 100I; 1002T, 496F

xmlproxy	152	S	1.3	4.7
updated	54	S	0.1	0.3
monitord	57	S	0.1	0.3
sys_monito	58	S	0.1	0.3
xmlproxy	56	S	0.0	8.2
alertmail	76	S	0.0	4.6
cli	396	S	0.0	1.2
cli	301	S	0.0	1.2
cmdbsvr	43	S	0.0	1.0
httpsd	147	S	0.0	1.0
cli	403	R	0.0	0.9
data_analy	60	S	0.0	0.6
httpsd	308	S	0.0	0.6
cli	379	S	0.0	0.5
hasync	63	S	0.0	0.4
hatalk	62	S	0.0	0.4
synconf	64	S	0.0	0.4
al_daemon	59	S	0.0	0.3
miglogd	53	S	0.0	0.3

The first line indicates the up time. The second line lists the processor and memory usage, where the parameters from left to right mean:

- U — Percent of user CPU usage (in this case 0%)
- S — Percent of system CPU usage (in this case 0%)
- I — Percentage of CPU idle (in this case 100%)
- T — Total memory in kilobytes (in this case 2008 KB)
- F — Available memory in kilobytes (in this case 445 KB)

The five columns of data provide the process name (such as `updated`), the process ID (`pid`), the running status, the CPU usage, and the memory usage. The status values are:

- S — Sleeping (idle)
- R — Running
- Z — Zombie (crashed)
- < — High priority
- N — Low priority

Related topics

- [diagnose system kill](#)
- [diagnose hardware cpu](#)
- [diagnose hardware mem](#)
- [get system performance](#)

execute

The `execute` command has an immediate and decisive effect on your FortiWeb appliance and, for that reason, should be used with care. Unlike `config` commands, most `execute` commands do not result in any configuration change.

This chapter describes the following commands:

<code>execute backup cli-config</code>	<code>execute ha manage</code>	<code>execute restore</code>
<code>execute backup full-config</code>	<code>execute ha synchronize</code>	<code>secondary-image</code>
<code>execute create-raid level</code>	<code>execute ping</code>	<code>execute shutdown</code>
<code>execute create-raid rebuild</code>	<code>execute ping6</code>	<code>execute telnet</code>
<code>execute date</code>	<code>execute ping-options</code>	<code>execute telnettest</code>
<code>execute db rebuild</code>	<code>execute ping6-options</code>	<code>execute time</code>
<code>execute factoryreset</code>	<code>execute reboot</code>	<code>execute traceroute</code>
<code>execute formatlogdisk</code>	<code>execute restore config</code>	<code>execute update-now</code>
<code>execute ha disconnect</code>	<code>execute restore image</code>	

backup cli-config

Use this command to manually back up the configuration file to a TFTP server.



This method does **not** include uploaded files such as:

- private keys
- certificates
- error pages
- WSDL files
- W3C Schema
- vulnerability scan settings

If your configuration has these files, use either a full TFTP or FTP/SFTP backup instead. See [“backup full-config” on page 510](#) or [“config system backup” on page 185](#).



This command does **not** include settings that remain at their default values for the currently installed version of the firmware. If you require a backup that includes those settings, instead use [“execute backup full-config” on page 510](#).

Alternatively, you can back up the configuration to an FTP or SFTP server. See [“config system backup” on page 185](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute backup cli-config tftp <filename_str> <tftp_ipv4> {entire | profile} [<password_str>]
```

Variable	Description	Default
<filename_str>	Type the name of the file to be used for the backup file, such as <code>FortiWeb_backup.conf</code> .	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.

Variable	Description	Default
{entire profile}	<p>Select either:</p> <ul style="list-style-type: none"> <code>entire</code> — Back up the core configuration file only. Note: This is not literally the entire configuration. It only contains the core configuration file, comprised of a CLI script. It does not include uploaded files such as error pages and private keys. <code>profile</code> — Back up only the web protection profiles. 	
[<password_str>]	<p>Type a password for use when encrypting the backup file using 128-bit AES.</p> <p>If you do not provide a password, the backup file will be stored as clear text.</p> <p>Caution: Remember the password or keep it in a secure location. You will be required to enter the same password when restoring an encrypted backup file. If you forget or lose the password, you will not be able to use that encrypted backup file.</p>	No default.

Example

This example uploads the FortiWeb appliance's system configuration to a file named `fweb.cfg` on a TFTP server at IP address 192.168.1.23. The file will not be password-encrypted.

```
execute backup cli-config tftp fweb.cfg 192.168.1.23 entire
```

Related topics

- [execute backup full-config](#)
- [execute restore config](#)
- [config system backup](#)

backup full-config

Use this command to manually back up the entire configuration file, **including** those settings that remain at their default values, to a TFTP server.



Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location. This backup method includes sensitive data such as your HTTPS certificates' private keys. Unauthorized access to private keys compromises the security of all HTTPS requests using those certificates.

Alternatively, you can back up the configuration to an FTP or SFTP server. See [“system backup” on page 185](#).

This backup includes settings that remain at their default values increases the file size of the backup, but may be useful in some cases, such as when you want to compare the default settings with settings that you have configured.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute backup full-config tftp <filename_str> <tftp_ipv4>  
[<password_str>]
```

Variable	Description	Default
<filename_str>	Type the name of the file to be used for the backup file, such as <code>FortiWeb_backup.conf</code> .	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.
[<password_str>]	Type a password for use when encrypting the backup file using 128-bit AES. If you do not provide a password, the backup file will be stored as clear text. Caution: Remember the password or keep it in a secure location. You will be required to enter the same password when restoring an encrypted backup file. If you forget or lose the password, you will not be able to use that encrypted backup file.	No default.

Example

This example uploads the FortiWeb appliance's entire configuration, including uploaded error page and HTTPS certificate files, to a file named `fweb.cfg` on a TFTP server at IP address 192.168.1.23. The file is encrypted with the password `P@ssword1`.

```
execute backup full-config tftp fweb.cfg 192.168.1.23 P@ssword1
```

Related topics

- [execute backup cli-config](#)
- [config system backup](#)

create-raid level

Use the this command to initialize the RAID.

Currently, only RAID level 1 is supported, and only on FortiWeb-1000B, 1000C, and 3000C/CFsx shipped with FortiWeb 4.0 MR1 or later.

On older appliances that have been upgraded to FortiWeb 4.0 MR1, RAID cannot be activated.



Back up any data before initializing the array.

Back up the data regularly. RAID is not a substitute for regular backups. RAID 1 (mirroring) is designed to improve hardware fault tolerance, but cannot negate all risks.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute create-raid level {raid1}
```

Variable	Description	Default
level {raid1}	Type the RAID level. Currently, only RAID level 1 is supported.	raid1

Related topics

- [config system raid](#)
- [diagnose hardware raid list](#)
- [execute create-raid rebuild](#)

create-raid rebuild

Use the this command to rebuild the RAID.

Currently, only RAID level 1 is supported, and only on FortiWeb-1000B, 1000C, and 3000C/CFsx shipped with FortiWeb 4.0 MR1 or later.

On older appliances that have been upgraded to FortiWeb 4.0 MR1, RAID cannot be activated.



Back up the data regularly. RAID is not a substitute for regular backups. RAID 1 (mirroring) is designed to improve hardware fault tolerance, but cannot negate all risks.

Rebuilding the array due to disk failure may result in some loss of packet log data.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute create-raid rebuild
```

Example

This example rebuilds the RAID array.

```
execute create-raid rebuild
```

The CLI displays the following:

```
This operation will clear all data on disk :0!  
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays additional messages.

Related topics

- [config system raid](#)
- [diagnose hardware raid list](#)

date

Use this command to display or set the system date.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute date [<date_str>]
```

Variable	Description	Default
date [<date_str>]	Type the current date for the FortiWeb appliance's time zone, using the format <code>yyyy-mm-dd</code> , where: <ul style="list-style-type: none"><code>yyyy</code> is the year. Valid years are 2001 to 2037.<code>mm</code> is the month. Valid months are 01 to 12.<code>dd</code> is the day of the month. Valid days are 01 to 31. If you do not specify a date, the command returns the current system date. Shortened values, such as <code>06</code> instead of <code>2006</code> for the year or <code>1</code> instead of <code>01</code> for the month or day, are not valid.	No default.

Example

This example sets the date to 17 September 2011:

```
execute date 2011-09-17
```

Related topics

- [execute time](#)
- [config system global](#)

db rebuild

Use this command to rebuild the FortiWeb appliance's internal database that it uses to store log messages.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute db rebuild
```

Related topics

- [execute formatlogdisk](#)
- [diagnose debug application miglogd](#)
- [diagnose debug upload](#)

factoryreset

Use this command to reset the FortiWeb appliance to its default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings.



Back up your configuration first. This command resets all changes that you have made to the FortiWeb appliance's configuration file and reverts the system to the default values for the firmware version. Depending on the firmware version, this could include factory default settings for the IP addresses of network interfaces. For information on creating a backup, see [“execute backup cli-config” on page 508](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute factoryreset
```

Related topics

- [execute backup cli-config](#)
- [execute backup full-config](#)
- [execute restore config](#)

formatlogdisk

Use this command to clear the logs from the FortiWeb appliance's hard disk and reformat the disk.



This operation deletes all locally stored log files.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

When you execute this command, the FortiWeb appliance displays the following message:

```
This operation will clear all data on the log disk and take a few
minutes according to the disk size!!
Do you want to continue? (y/n)
```

Syntax

```
execute formatlogdisk
```

Related topics

- [execute db rebuild](#)

ha disconnect

Use this command to manually force a FortiWeb appliance to leave the HA group, **without** unplugging any cables. This can be useful, for example, if you need to remove a standby appliance from the HA cluster in order to configure it for standalone operation, and want to do so **without** disrupting traffic, and without unplugging cables.

Behavior varies by which appliance you eject:

- **Active** — Failover occurs. The standby remains as a member of the HA group, and will elect itself as the new active appliance, assuming all of the HA cluster's configured IP addresses and traffic processing duties.
- **Standby** — No failover occurs. The active appliance remains actively processing traffic.

To ensure that you can re-connect to the ejected appliance's GUI or CLI via a remote network connection (not only via its local console), this command requires that you specify an IP address and port name that will become its new management interface. By default, it will be accessible via HTTP, HTTPS, SSH, and telnet. (All other network interfaces on the ejected appliance will be brought down and reset to 0.0.0.0/0.0.0.0. To configure them, you must connect to the ejected appliance's GUI or CLI.)

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
execute ha disconnect <serial-number_str> <interface_name>  
<interface_ipv4mask>
```

Variable	Description	Default
disconnect <serial-number_str>	Type the serial number of the FortiWeb appliance that you want to disconnect from the cluster. To display the serial number of each appliance in the HA group, type: execute ha disconnect ?	No default.
<interface_name>	Type the name of the network interface, such as <code>port1</code> , that will be configured as the ejected appliance's management interface.	No default.
<interface_ipv4mask>	Type the IP address and netmask that will be configured as the ejected appliance's management interface.	No default.

Example

This example ejects the standby appliance whose serial number is FV-1KC3R11111111, assigning its `port1` to be the web UI/GUI interface, reachable at 10.0.0.1.

```
execute ha disconnect FV-1KC3R11111111 port1 10.0.0.1/24
```

After the command completes, to reconfigure the ejected appliance, you could then use either a web browser or SSH client to connect to 10.0.0.1 in order to reconfigure it for standalone operation.

Related topics

- [execute ha disconnect](#)
- [execute ha manage](#)
- [diagnose system ha status](#)
- [diagnose system ha mac](#)
- [get system status](#)
- [config system global](#)

ha manage

Use this command to set the device priority of a standby appliance in the HA group.

If the HA cluster is configured to override uptime and consider the device priority first, this can cause the HA cluster to failover to a new active appliance (whichever appliance has a smaller device priority number). Triggering a failover can be useful if, for example, you need to connect to the web UI of the standby FortiWeb in order to view its log messages.



Unlike on FortiGate appliances, this command does **not** connect you to another appliance in the HA group via the HA link. To connect to the standby appliance, either use a local console, or switch the roles of the main and standby appliance so that you can connect to the former standby through the network, while it is acting as main.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute ha manage <serial-number_str> <priority_int>
```

Variable	Description	Default
manage <serial-number_str> >	Type the serial number of the FortiWeb appliance whose device priority you want to configure. To display the serial number of the standby, type: execute ha manage ?	No default.
<priority_int>	Type the device priority number. Smaller device priority numbers indicate higher priority. The appliance with the smallest number will usually become the active appliance. For details, see the FortiWeb Administration Guide . The valid range is from 0 to 9.	No default.

Example

This example sets the device priority of the standby appliance to 4. Since the device priority of the active appliance is 5, the standby appliance now has a greater device priority (smaller number). If the device priority override is enabled, this causes a failover to occur, and FV-1KC3R11111111 becomes the new active appliance.

```
execute ha manage FV-1KC3R11111111 4
```

Related topics

- [execute ha disconnect](#)
- [execute ha synchronize](#)
- [diagnose system ha status](#)
- [diagnose system ha mac](#)
- [config system global](#)

ha synchronize

Use this command to manually control the synchronization of configuration files and FortiGuard service-related packages from the active HA appliance to the standby appliance.

Typically, most HA synchronization happens automatically, whenever changes are made. However, in some cases, you may want to use this command to manually initiate full or partial HA synchronization.

- To delay synchronization to a more convenient time if you are planning to make large batch changes, and therefore delayed synchronization is preferable for network performance reasons
- To manually force synchronization of files that are not automatically synchronized
- To trigger automatic synchronization if it has been interrupted due to HA link failure, daemon crashes, etc.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute ha synchronize {avupd | irdb | config | geodb | waf}
```

```
execute ha synchronize {start | stop}
```

Variable	Description	Default
synchronize {avupd irdb config geodb waf}	Select which part of the configuration and/or FortiGuard service-related packages to synchronize. <ul style="list-style-type: none">• <code>avupd</code> — Only the FortiGuard Antivirus service package, including the virus signatures, scan engine, and proxy. <i>This file is not automatically synchronized due to its large size</i>, but HA synchronization can be manually forced via this command.• <code>irdb</code> — Only the IP Reputation Database (IRDB).• <code>config</code> — Only the core CLI configuration file (<code>fwb_system.conf</code>) and auxiliary files such as X.509 certificates. Does <i>not</i> include FortiGuard packages.• <code>geodb</code> — Only the geography-to-IP address mappings. Similar to firmware, these can be downloaded from the Fortinet Technical Support web site. <i>This file is not automatically synchronized due to its large size</i>, but HA synchronization can be manually forced via this command.• <code>waf</code> — Entire configuration, including CLI configuration, system files, and databases. Note: This command has no effect if you use the command <code>execute ha synchronize stop</code> to pause it manually.	No default.
synchronize {start stop}	Select whether to start or stop synchronization.	No default.

Example

This example shows how to manually synchronize the virus signature and engine package to the standby appliance.

```
FortiWeb # execute ha synchronize avupd  
starting synchronize with HA master...
```

Related topics

- [execute ha disconnect](#)
- [execute ha manage](#)
- [config system global](#)

ping

Use this command to perform an ICMP `ECHO` request (also called a ping) to a host by specifying its fully qualified domain name (FQDN) or IPv4 address, using the options configured by [execute ping-options](#).

Pings are often used to test IP-layer connectivity during troubleshooting.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
execute ping {<host_fqdn> | <host_ipv4>}
```

Variable	Description	Default
ping {<host_fqdn> <host_ipv4>}	Type either the IPv4 address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example pings a host with the IP address 172.16.1.10.

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.16.1.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results indicate that a route exists between the FortiWeb appliance and 172.16.1.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds.

Example

This example pings a host with the IP address 10.0.0.1.

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds, no output appears. The administrator halts the ping by pressing Ctrl+C. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results indicate the host may be down, or there is no route between the FortiWeb appliance and 10.0.0.1. To determine the point of failure along the route, further diagnostic tests are required, such as [“execute traceroute” on page 538](#).

Related topics

- [config system interface](#)
- [config server-policy vserver](#)
- [execute ping-options](#)
- [execute ping6](#)
- [execute telnettest](#)
- [execute traceroute](#)
- [diagnose network ip](#)
- [diagnose hardware nic](#)
- [diagnose network sniffer](#)
-

ping6

Use this command to perform an ICMP `ECHO` request (also called a ping) to a host by specifying its IPv6 address, using the options configured by [“execute ping-options” on page 525](#).

Pings are often used to test IP-layer connectivity during troubleshooting.

To use this command, your administrator account’s access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute ping6 {<host_fqdn> | <host_ipv6>}
```

Variable	Description	Default
ping6 {<host_fqdn> <host_ipv6>}	Type either the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example pings a host with the IP address 2001:0db8:85a3::8a2e:0370:7334.

```
execute ping6 2607:f0b0:f:420::
```

The CLI displays the following:

```
PING 2607:f0b0:f:420:: (2607:f0b0:f:420::): 56 data bytes
```

After several seconds, no output appears. The administrator halts the ping by pressing Ctrl+C. The CLI displays the following:

```
--- 2607:f0b0:f:420:: ping statistics ---  
5 packets transmitted, 0 packets received, 100% packet loss
```

The results indicate the host may be down, or there is no route between the FortiWeb appliance and 2607:f0b0:f:420::. To determine the point of failure along the route, further diagnostic tests are required, such as [“execute traceroute” on page 538](#).

Related topics

- [config system interface](#)
- [config server-policy vserver](#)
- [execute ping6-options](#)
- [execute telnettest](#)
- [execute traceroute](#)
- [diagnose network ip](#)
- [diagnose hardware nic](#)
- [diagnose network route](#)
- [diagnose network sniffer](#)

ping-options

Use these commands to configure the behavior of the `execute ping` command.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute ping-options data-size <bytes_int>
execute ping-options df-bit {yes | no}
execute ping-options pattern <bufferpattern_hex>
execute ping-options repeat-count <repeat_int>
execute ping-options source {auto | <interface_ipv4>}
execute ping-options timeout <seconds_int>
execute ping-options tos {<service_type>}
execute ping-options ttl <hops_int>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes. This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure <code>pattern <bufferpattern_hex></code> .	56
df-bit {yes no}	Enter either <code>yes</code> to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter <code>no</code> to allow the ICMP packet to be fragmented.	no
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as <code>00ffaabb</code> , to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by <code>data-size <bytes_int></code> .	No default.
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto <interface_ipv4>}	Select the network interface from which the ping is sent. Enter either <code>auto</code> or a FortiWeb network interface IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2
tos {<service_type>}	Enter the IP type-of-service option value, either: <ul style="list-style-type: none"><code>default</code> — Do not indicate. (That is, set the TOS byte to 0.)<code>lowcost</code> — Minimize cost.<code>lowdelay</code> — Minimize delay.<code>reliability</code> — Maximize reliability.<code>throughput</code> — Maximize throughput.	default

Variable	Description	Default
ttl <hops_int>	Enter the time-to-live (TTL) value.	64
validate-reply {yes no}	Select whether or not to validate ping replies.	no
view-settings	Display the current ping option settings.	No default.

Example

This example sets the number of pings to three and the source IP address to 10.10.10.1, then views the ping options to verify their configuration.

```
execute ping-option repeat-count 3
execute ping-option source 10.10.10.1
execute ping-option view-settings
```

The CLI would display the following:

```
Ping Options:
  Repeat Count: 3
  Data Size: 56
  Timeout: 2
  TTL: 64
  TOS: 0
  DF bit: unset
  Source Address: 10.10.10.1
  Pattern:
  Pattern Size in Bytes: 0
  Validate Reply: no
```

Related topics

- [execute ping](#)
- [execute traceroute](#)

ping6-options

Use these commands to configure the behavior of the `execute ping6` command.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute ping6-options data-size <bytes_int>
execute ping6-options pattern <bufferpattern_hex>
execute ping6-options repeat-count <repeat_int>
execute ping6-options source {auto | <interface_ipv4>}
execute ping6-options timeout <seconds_int>
execute ping6-options tos {<service_type>}
execute ping6-options ttl <hops_int>
execute ping6-options validate-reply {yes | no}
execute ping6-options view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes. This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure <code>pattern <bufferpattern_hex></code> .	56
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as 00ffaabb, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by <code>data-size <bytes_int></code> .	No default.
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto <interface_ipv6>}	Select the network interface from which the ping is sent. Enter either <code>auto</code> or a FortiWeb network interface IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2
tos {<service_type>}	Enter the IP type-of-service option value, either: <ul style="list-style-type: none">• <code>default</code> — Do not indicate. (That is, set the TOS byte to 0.)• <code>lowcost</code> — Minimize cost.• <code>lowdelay</code> — Minimize delay.• <code>reliability</code> — Maximize reliability.• <code>throughput</code> — Maximize throughput.	default
ttl <hops_int>	Enter the time-to-live (TTL) value.	64
validate-reply {yes no}	Select whether or not to validate ping replies.	no
view-settings	Display the current ping option settings.	No default.

Example

This example sets the number of pings to 3, then views the ping options to verify their configuration.

```
execute ping6-option repeat-count 3
execute ping6-option view-settings
```

The CLI would display the following:

```
IPV6 Ping Options:
  Repeat Count: 3
  Data Size: 56
  Timeout: 2
  Interval: 1
  TTL: 64
  TOS: 0
  Source Address: auto
  Pattern:
  Pattern Size in Bytes: 0
  Validate Reply: no
```

Related topics

- [execute ping6](#)
- [execute traceroute](#)

reboot

Use this command to restart the FortiWeb appliance.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute reboot
```

Example

This example shows the reboot command in action.

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !  
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages while the reboot is occurring.

If you are connected to the CLI through the network, the CLI will not display any notification while the reboot is occurring, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection is terminated. Time required by the reboot varies by many factors, such as whether or not hard disk verification is required, but may be several minutes.

Related topics

- [execute shutdown](#)
- [get system performance](#)

restore config

Use this command to restore the configuration from a configuration backup file on an TFTP server, or to install primary or backup firmware.



Back up the configuration before restoring the configuration. This command restores configuration changes only, and does not affect settings that remain at their default values. Default values may vary by firmware version. For backup commands, see [“execute backup cli-config” on page 508](#) and [“execute backup full-config” on page 510](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute restore config tftp <filename_str> <tftp_ipv4>
[<password_str>]
```

Variable	Description	Default
<filename_str>	Type the name of the backup or firmware image file.	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.
[<password_str>]	Type the password that was used to encrypt the backup file, if any. If you do not provide a password, the backup file must have been stored as clear text.	No default.

Example

This example downloads a configuration file named `backup.conf` from the TFTP server, 192.168.1.23, to the FortiWeb appliance. The backup file was encrypted with the password `P@ssword1`.

```
execute restore config tftp backup.conf 192.168.1.23 P@ssword1
```

The FortiWeb appliance then applies the configuration backup and reboots.

Related topics

- [execute backup full-config](#)
- [execute restore config](#)
- [execute restore image](#)
- [execute restore secondary-image](#)

restore image

Use this command to install firmware on the primary partition and reboot.



Back up the configuration before installing new firmware. Installing new firmware can change default settings and reset settings that are incompatible with the new version. For backup commands, see [“execute backup full-config” on page 510](#) and [“execute backup cli-config” on page 508](#).

Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiWeb appliance to its firmware/factory default configuration.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute restore image ftp <filename_str> <ftp_ipv4>
execute restore image tftp <filename_str> <tftp_ipv4>
```

Variable	Description	Default
<filename_str>	Type the name of the firmware image file.	No default.
<ftp_ipv4>	Type the IP address of the TFTP server.	No default.
<tftp_ipv4>	Type the IP address of the FTP server.	No default.

Example

This example installs a firmware file named `firmware.out` from the TFTP server, 192.168.1.23, to the FortiWeb appliance.

```
execute restore image tftp firmware.out 192.168.1.23
```

The FortiWeb appliance downloads the firmware file, installs it, and reboots.

Related topics

- [execute backup cli-config](#)
- [execute backup full-config](#)
- [execute restore config](#)
- [execute restore secondary-image](#)
- [diagnose system flash](#)
- [get system status](#)

restore secondary-image

Use this command to install backup firmware on the secondary partition and reboot.



Back up the configuration before installing new firmware. Installing new firmware can change default settings and reset settings that are incompatible with the new version. For backup commands, see [“execute backup full-config” on page 510](#) and [“execute backup cli-config” on page 508](#).

Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiWeb appliance to its firmware/factory default configuration.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute restore secondary-image ftp <filename_str> <ftp_ipv4>
execute restore secondary-image tftp <filename_str> <tftp_ipv4>
```

Variable	Description	Default
<filename_str>	Type the name of the firmware image file.	No default.
<ftp_ipv4>	Type the IP address of the FTP server.	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.

Example

This example installs a firmware file named `firmware.out` from the TFTP server, 192.168.1.23, to the FortiWeb appliance.

```
execute restore secondary-image tftp firmware.out 192.168.1.23
```

The FortiWeb appliance downloads the firmware file, installs it, and reboots.

Related topics

- [execute backup cli-config](#)
- [execute backup full-config](#)
- [execute restore config](#)
- [execute restore image](#)
- [diagnose system flash](#)
- [get system status](#)

shutdown

Use this command to prepare the FortiWeb appliance to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.



Power off the FortiWeb appliance only after issuing this command. Unplugging or switching off the FortiWeb appliance without issuing this command could result in data loss.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute shutdown
```

Example

This example shows the reboot command in action.

```
execute shutdown
```

The CLI displays the following:

```
This operation will halt the system
(power-cycle needed to restart)!Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is shutting down...(power-cycle needed to restart)
```

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI will not display any notification when the shutdown is complete, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection times out.

Related topics

- [execute reboot](#)

telnet

Use this command to open a Telnet connection to a server. using IPv4 to port 23.



Telnet connections are not secure. Eavesdroppers could easily obtain your administrator password. Only use telnet over a trusted, physically secured network, such as a direct connection between your computer and the appliance.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute telnet <host_ipv4>
```

Variable	Description	Default
telnet <host_ipv4>	Type the IP address of the host.	No default.

Example

This example Telnets to a host with the IP address 172.16.1.10.

```
execute telnet 172.16.1.10
login: admin
Password: *****
```

Related topics

- [execute telnettest](#)
- [execute ping](#)
- [execute ping6](#)

telnettest

Use this command to open a Telnet connection to a server using IPv4 or IPv6, and either. This can be useful when troubleshooting if, for example, the server may not support HTTP versions, methods, headers, etc. being used by the client.



Telnet connections are not secure. Eavesdroppers could easily obtain your administrator password. Only use Telnet over a trusted, physically secured network, such as a direct connection between your computer and the appliance, and from the appliance to the server.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute telnettest {<host_ipv4> | <host_ipv6>}
```

Variable	Description	Default
telnettest {<host_ipv4> <host_ipv6>}	Type the IP address of the host.	No default.

Example

This example Telnets to a host with the IPv4 address 172.16.1.10 on port 80, the IANA standard port for HTTP.

```
FortiWeb# exec telnettest 172.16.1.10:80
```

```
Connected
```

```
GET /
```

```
Entering interactive mode. Type CTRL-D to exit.
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

```
<html><head>
```

```
<title>501 Method Not Implemented</title>
```

```
</head><body>
```

```
<h1>Method Not Implemented</h1>
```

```
<p>Get to /index.html not supported.<br />
```

```
</p>
```

```
<hr>
```

```
<address>Apache/2.2.22 (Unix) DAV/2 mod_ssl/2.2.22 OpenSSL/0.9.8x  
Server at irene.local Port 80</address>
```

```
</body></html>
```

```
Connection closed.
```

```
Connection status to 172.16.1.10 port 80:
```

```
Connecting to remote host succeeded.
```

Related topics

- [execute telnet](#)
- [execute ping](#)
- [execute ping6](#)

time

Use this command to display or set the system time.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute time [<time_str>]
```

Variable	Description	Default
time [<time_str>]	<p>Type the current date for the FortiWeb appliance's time zone, using the format <code>hh:mm:ss</code>, where:</p> <ul style="list-style-type: none">• <code>hh</code> is the hour. Valid hours are 00 to 23.• <code>mm</code> is the minute. Valid minutes are 00 to 59.• <code>ss</code> is the second. Valid seconds are 00 to 59. <p>If you do not specify a time, the command returns the current system time.</p> <p>Shortened values, such as 1 instead of 01 for the hour, are valid. For example, you could enter either <code>01:01:01</code> or <code>1:1:1</code>.</p>	No default.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

Related topics

- [execute date](#)
- [config system global](#)

traceroute

Use this command to use ICMP to test the connection between the FortiWeb appliance and another network device, and display information about the time required for network hops between the device and the FortiWeb appliance.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see [“Permissions” on page 47](#).

Syntax

```
execute traceroute {<host_fqdn> | <host_ipv4>}
```

Variable	Description	Default
traceroute {<host_fqdn> <host_ipv4>}	Type either the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example tests connectivity between the FortiWeb appliance and docs.fortinet.com. In this example, the trace times out after the first hop, indicating a possible connectivity problem at that point in the network.

```
FortiWeb# execute traceroute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte packets
 1  172.16.1.200 (172.16.1.200)  0.324 ms  0.427 ms  0.360 ms
 2  * * *
```

Example

This example tests the availability of a network route to the server example.com.

```
execute traceroute example.com
```

The CLI displays the following:

```
traceroute to example.com (192.168.1.10), 32 hops max, 72 byte packets
 1  172.16.1.2    0 ms  0 ms  0 ms
 2  10.10.10.1    <static.isp.example.net>  2 ms  1 ms  2 ms
 3  10.20.20.1    1 ms   5 ms  1 ms
 4  10.10.10.2    <core.isp.example.net>  171 ms  186 ms  14 ms
 5  10.30.30.1    <isp2.example.net>  10 ms  11 ms  10 ms
 6  10.40.40.1    73 ms  74 ms  75 ms
 7  192.168.1.1   79 ms  77 ms  79 ms
 8  192.168.1.2   73 ms  73 ms  79 ms
 9  192.168.1.10  73 ms  73 ms  79 ms
10  192.168.1.10  73 ms  73 ms  79 ms
```

Example

This example attempts to test connectivity between the FortiWeb appliance and example.com. However, the FortiWeb appliance could not trace the route, because the primary or secondary DNS server that the FortiWeb appliance is configured to query could not resolve the FQDN example.com into an IP address, and it therefore did not know to which IP address it should connect. As a result, an error message is displayed.

```
FortiWeb# execute traceroute example.com  
traceroute: unknown host example.com  
Command fail. Return code 1
```

To resolve the error message in order to perform connectivity testing, the administrator would first configure the FortiWeb appliance with the IP addresses of DNS servers that can resolve the FQDN example.com. For details, see [“config system dns” on page 201](#).

Related topics

- [execute ping](#)
- [execute ping-options](#)
- [diagnose network ip](#)
- [diagnose hardware nic](#)
- [diagnose network sniffer](#)

update-now

Use this command to initiate an update of the predefined robots, data types, suspicious URLs, and attack signatures used by your FortiWeb appliance.

FortiWeb appliances receive updates from the FortiGuard Distribution Network (FDN). The FDN is a world-wide network of FortiGuard Distribution Servers (FDS). FortiWeb appliances connect to the FDN by connecting to the FDS nearest to the FortiWeb appliance by its configured time zone.

The time required for the update varies with the availability of the updates, the size of the updates, and the speed of the FortiWeb appliance's network connection. If event logging is enabled, and the FortiWeb appliance cannot connect successfully, it will log the message `update failed, failed to connect any fds servers! or FortiWeb is unauthorized`

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see ["Permissions" on page 47](#).

Syntax

```
execute update-now
```

get

The `get` command displays parts of your FortiWeb appliance's configuration in the form of a list of settings and their values.

Unlike `show`, `get` displays **all** settings, even if they are still in their default state.

For example, you might get the current DNS settings:

```
get system dns
primary          : 172.16.95.19
secondary        : 0.0.0.0
domain           : example.com
```

Notice that the command displays the setting for the secondary DNS server, even though it has not been configured, or has reverted to its default value.

Also unlike `show`, unless used from within an object or table, `get` requires that you specify the object or table whose settings you want to display.

For example, at the root prompt, this command would be valid:

```
get system dns
```

and this command would **not** be valid:

```
get
```

Like `show`, depending on whether or not you have specified an object, `get` may display one of two different outputs, either the configuration:

- that you have just entered but not yet saved, or
- as it currently exists on the flash disk, respectively.

For example, immediately after configuring the secondary DNS server setting but **before** saving it, `get` displays two different outputs (differences highlighted in bold):

```
FortiWeb# config system dns
FortiWeb (dns)# set secondary 192.168.1.10
FortiWeb (dns)# get
primary          : 172.16.95.19
secondary       : 192.168.1.10
domain           : example.com
FortiWeb (dns)# get system dns
primary          : 172.16.95.19
secondary       : 0.0.0.0
domain           : example.com
```

The first output from `get` indicates the value that you have configured but not yet saved; the second output from `get` indicates the value that was last saved to disk.

If you were to now enter `end`, saving your setting to disk, `get` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently

entered secondary DNS setting instead of saving it to disk, the FortiWeb appliance's configuration would therefore match the second output, not the first.



If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `get`, with and without the object name, can be a useful way to remind yourself.

Most `get` commands, such as `get system dns`, are used to display configured settings. You can find relevant information about such commands in the corresponding `config` commands in the `config` chapter.

Other `get` commands, such as `get system performance`, are used to display system information that is **not** configurable. This chapter describes this type of `get` command.

The `get` commands require at least read (r) permission to applicable administrator profile groups.

This chapter describes the following commands.

`get router all`

`get system performance`

`get system status`

`get system logged-users`



Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see “[config](#)” on [page 62](#).



When ADOMs are enabled, and if you log in as `admin`, the top level of the shell changes: the two top level items are `get global` and `get vdom`.

- `get global` displays settings that only `admin` or other accounts with the *prof_admin* access profile can change.
- `get vdom` displays each ADOM and its respective settings.

This menu and CLI structure change is not visible to non-global accounts; ADOM administrators' navigation menus continue to appear similar to when ADOMs are disabled, except that global settings such as network interfaces, HA, and other global settings do not appear.

router all

Use this command to display the list of configured and implied static routes.

Syntax

```
get router all
```

Example

```
get router all
```

Output such as the following appears in the CLI. In this case, only 172.20.120.0 was a static route configured by an administrator using [config router static](#). The other routes are implied by the IP addresses of the virtual servers (10.1.1.10 listening on port2) and network interfaces (192.168.1.25 for port3).

IP Device	Mask	Gateway	Distance
172.20.120.0 port1	255.255.255.0	0.0.0.0	0
10.1.1.221 port2	255.255.255.255	0.0.0.0	0
192.168.1.0 port3	255.255.255.0	0.0.0.0	0

Related topics

- [config router static](#)
- [diagnose network route](#)

system logged-users

Lists which administrator accounts are currently logged in to the FortiWeb appliance via the local console, web UI, or CLI (including through the JavaScript-based *CLI Console* widget of the web UI). It also displays the login time of that administrative session.

For information on allowing only one administrator to be logged in at any given time, see [“config system global” on page 206](#).

Syntax

```
get system logged-users
```

Example

```
get system logged-users
Logged in users: 2
INDEX USERNAME          TYPE  FROM                TIME
    0 admin              cli   console             Thu Jun 21 14:50:09
2012
    1 admin              cli   ssh(172.20.120.225) Thu Jun 21 15:19:09
2012
```

Related topics

- [config system admin](#)
- [config system global](#)

system performance

Displays the FortiWeb appliance's CPU usage, memory usage, average system load, and up time.

Normal idle load varies by hardware platform, firmware, and configured features. To determine your specific baseline for idle, configure your system completely, reboot, then view the system load. After at least 1 week of uptime with typical traffic volume, view the system load again to determine the normal non-idle baseline.

System load is the average of percentages relative to the maximum possible capability of this FortiWeb appliance's hardware. It includes:

- average system load
- number of HTTP daemon/proxy processes or children
- memory usage
- disk swap usage

Syntax

```
get system performance
```

Example

```
FortiWeb # get system performance
CPU states:      4% used, 96% idle
Memory states: 18% used
System Load:    1
Up:              28 days, 11 hours, 38 minutes
```

Related topics

- [get system status](#)
- [diagnose hardware cpu](#)
- [diagnose hardware mem](#)
- [diagnose hardware raid list](#)
- [diagnose system kill](#)
- [diagnose system top](#)
- [diagnose policy](#)
- [execute reboot](#)

system status

Use this command to display system status information including:

- FortiWeb firmware version, build number and date
- FortiWeb appliance serial number and boot loader (“Bios”) version
- log hard disk availability
- host name
- operation mode, such as reverse proxy or transparent inspection
- current HA status for all appliances in the HA cluster (if HA is enabled)

Syntax

```
get system status
```

Example

```
get system status
International Version:FortiWeb-1000C 5.01,build0039,130726
Serial-Number:FV-1KC3R11700094
Bios version:04000002
Log hard disk:Available
Hostname:FortiWeb
Operation Mode:Reverse Proxy
Current HA mode=active-passive, Status=main
HA member :
  Serial-Number      Priority  HA-Role
  FV-1KC3R11700136   5        standby
  FV-1KC3R11700094   1        main
```

Related topics

- [get system performance](#)
- [diagnose system ha status](#)
- [config system global](#)

show

The `show` command displays parts of your FortiWeb appliance's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.

The `show` commands require at least read (r) permission to applicable administrator profile groups.



Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see “[config](#)” on [page 62](#).

Unlike `get`, `show` does **not** display settings that are assumed to remain in their default state.

For example, you might show the current DNS settings:

```
FortiWeb# show system dns
config system dns
    set primary 172.16.1.10
    set domain "example.com"
end
```

Notice that the command does **not** display the setting for the secondary DNS server. This indicates that it has not been configured, or has reverted to its default value.

Like `get`, depending on whether or not you have specified an object, `show` may display one of two different outputs, either the configuration:

- that you have just entered but not yet saved, or
- as it currently exists on the flash disk, respectively.

For example, immediately after configuring the secondary DNS server setting but **before** saving it, `show` displays two different outputs (differences highlighted in bold):

```
FortiWeb# config system dns
FortiWeb (dns)# set secondary 192.168.1.10
FortiWeb (dns)# show
config system dns
    set primary 172.16.1.10
    set secondary 192.168.1.10
    set domain "example.com"
end
FortiWeb (end)# show system dns
config system dns
    set primary 172.16.1.10
    set domain "example.com"
end
```

The first output from `show` indicates the value that you have configured but not yet saved; the second output from `show` indicates the value that was last saved to disk.



If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `show`, with and without the object name, can be a useful way to remind yourself.

If you were to now enter `end`, saving your setting to disk, `show` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently entered secondary DNS setting instead of saving it to disk, the FortiWeb appliance's configuration would therefore match the second output, not the first.



When ADOMs are enabled, and if you log in as `admin`, the top level of the shell changes: the two top level items are `show global` and `show vdom`.

- `show global` displays settings that only `admin` or other accounts with the *prof_admin* access profile can change.
- `show vdom` displays each ADOM and its respective settings.

This menu and CLI structure change is not visible to non-global accounts; ADOM administrators' navigation menus continue to appear similar to when ADOMs are disabled, except that global settings such as network interfaces, HA, and other global settings do not appear.

Index

Numerics

127.0.0.1 483
200 OK 119
301 Moved Permanently 382
302 Moved Temporarily 382
3DES 37, 177
403 Forbidden 283, 304, 328, 333, 359, 369, 380, 382, 395, 398, 411
404 File Not Found 398
70007 336

A

abort 46
accept 275, 283, 304, 314, 322, 325, 328, 333, 340, 343, 358, 369, 393, 394, 408
Accept: 276
access control
 protected web sites 273, 350
 web UI 167
access profile 47, 49, 167, 171
ACK 119
action message format (AMF) 392, 408
Active Directory 251, 363
active-passive 213, 214
address resolution protocol (ARP) 216
 extra packets 216
 gratuitous 216
 table 480
admin 35, 49
administrator
 access, restricting 170, 172, 173, 222, 223
 domain (ADOM) 57, 172
 logged in 544
 netmask 172, 173
 password 172
 simultaneous sessions 210
Adobe
 Flash 355, 392
 PDF 86, 297
AES 37, 177, 186, 509, 510
AJAX 392, 408
Akamai 414
alert email 64, 275, 283, 284, 293, 304, 314, 322, 325, 328, 333, 340, 343, 358, 359, 365, 369, 375, 393, 394, 408
 severity 284, 334, 337, 359, 375
allow 375
alphanumeric 134
ambiguous command 39, 51
anonymous 246
 FTP 186
 proxy 332

ANSI 133
 escape code 134
Apache 321
application-policy 108
ASCII 52, 53, 489
ASIC chip 204
attack
 BEAST 177
 block 275, 283, 293, 304, 314, 322, 325, 328, 333, 340, 343, 358, 369, 375, 393, 394, 408
 brute force login 269
 buffer overflow 319
 data leak 282
 denial of service (DoS) 175, 203, 339
 log 275, 283, 284, 304, 314, 322, 325, 328, 333, 334, 337, 340, 343, 358, 359, 365, 369, 375, 393, 394, 408
 redirect 283, 304, 328, 333, 359, 369
 signature 355
 spoofing 415
 XHTML parser 392, 408
 XML parser 392, 408
attribute
 CN 246
 group membership 246
 LDAP 246
 RADIUS 171, 252, 253
 XML 392, 408
auditor 167
authentication 252
 HTTP 249, 251, 254, 307, 310
 NTLM 251
 supporting modes 230, 231
authorization 252
Authorization: 365
auto-learning 168
 dynamic URLs 110
 parameter structures 110
auto-negotiation 475
availability 213

B

back trace 449
back-reference 113, 114
bank sort code 134
baseline 545
batch changes 34, 55
baud rate 55, 200
BCOPY 261, 263
BEAST 177
best practices 24
bind DN 247
BIOS 131, 132

bit
 strength 37, 186, 211, 509, 510

bits
 TOS 489

bits per second (bps) 35

black-listed IPs 332, 336, 337

block period 275, 283, 293, 304, 314, 322, 325, 328,
 333, 340, 343, 358, 369, 393, 394, 408

Blowfish 37

body rewrite 380

boot
 interrupt 34
 loader 546
 wait for HA heartbeat 218

botnet 332

bridge 204, 231, 241
 protocol data unit (BPDU) 241

broadcast 216, 475

browser 159

brute force login attack 269

buffer
 compression inspection 178
 decompression 178
 DLP scan 176
 HTTP parser 66
 length 319
 overflow 319
 RAM 472
 size 176
 terminal emulator 55

bypass 165
 during power outage 204

BZIP2 178

C

cache
 alignment 466
 ARP 480
 CPU 466
 hard disk 533
 RAM 472
 response 175
 route 485

capture group 113, 114

certificate 144, 157
 authority (CA) 150, 189, 191, 196
 backup 185, 186, 508, 510
 default 194
 local 194
 personal 150, 158
 revocation list (CRL) 150, 191, 196
 server 194
 signing chain 159
 trust 159
 user 150, 158
 warning 159

chain of trust 159

character
 encoding 175

checksum 433
 header 489

CIDR 43

cipher 37
 block chaining (CBC) 177

Cisco discovery protocol (CDP) 220

Citrix
 Receiver 101

cloaking 283, 358, 380

cluster 213, 502

cmdbsvr 506

collision 474, 475

color code 133

command 39
 abbreviation 51
 ambiguous 39, 51
 CLI Console widget 35, 544
 completion 50
 constraints 25
 help 50
 incomplete 39
 interactive 51
 line interface (CLI) 23, 170
 multi-line 39, 51
 prompt 44, 50, 54, 200, 208
 scope 39, 40
 syntax 25, 38

comma-separated value (CSV) format 95, 134

common name (CN) 246

compress files 288
 exception 286

compression 288

config 62, 167

configuration management database (CMDB) 446

configuration script 34

CONNECT 183

connection
 limits 313
 persistence 147
 reset 144
 trace 487

Connection: 146

console port 34, 35

constraint
 CLI 25, 38
 web page input 327

content routing 143

Content-Length: 321

Content-Type: 289, 385

conventions 23

Cookie 285

cookie 393, 396
 limit 320
 support 313, 410

Cookie: 176
 buffer 176

core dump 503

country 299
 code 131, 132

- cp1252 53
- CP7 chip 204
- CPU
 - and ASIC chip 204
 - cache 466
 - cores 466
 - intensive 178
 - load
 - process/thread 545
 - usage 236, 466, 505, 506, 545
- crash log 449
- credit card number 131, 132, 134
- cross-site request forgery (CSRF) 350
- cross-site scripting (XSS) 181, 355, 392, 408
 - prevented on the FortiWeb itself 51
- custom
 - access header 276
 - application 108, 110
 - attack signature 207, 282
 - auto-learning
 - application 108, 110
 - data leak signature 282
 - data type 67, 124, 330
 - error page 117
 - network service 148, 162
 - report
 - footer 85
 - logo 85
 - rule
 - access 272, 273
 - logging only non-sensitive data 67, 92
 - suspicious request URLs 127
 - URL interpreter 111
- customer service 23

D

- Danish postnumre 131, 132
- dashboard 498
- data
 - leak 355
 - signature 282
 - loss 24
 - system 513
 - type 124
 - autolearning 387
 - CLI 40
 - group 130
 - predefined 181
 - updates 181
- data-size
 - execute ping-options 525, 527
- date
 - in request/response 131, 132
 - system 210
- daylight savings time (DST) 207
- DB-9 34
- debug log 424
- debug_info 460

- default
 - access profile 167
 - administrator account 35, 49
 - ADOM 60
 - gateway 103
 - password 23, 35
 - route 103
 - values 510
- delete
 - cannot 167
- denial of service (DoS) 175, 203, 321, 339
 - protection 265, 324, 339
- deny 275, 283, 293, 304, 314, 322, 325, 328, 333, 340, 343, 358, 369, 375, 393, 394, 408
- df-bit
 - execute ping-options 525
- diagnose 423, 487
- differentiated services code point (DSCP) 489
- Diffie-Hellman exchange 160
- disk
 - capacity 468
 - flash 468
 - format 516
 - swap 545
 - usage 504
- display refresh rate 206
- distinguished name (DN) 246
- document
 - conventions 23
 - object model (DOM) 302
- domain
 - administrative (ADOM) 57
- domain name
 - allowed in HTTP requests 105, 106
 - email server 73
 - FDN 180
 - FTP server 187
 - local 201
 - NTP server 210
 - resolution 201
 - rewrite 383
 - service (DNS)
 - reverse 376
 - server 201
 - web proxy 183
 - web server 115, 257
- dotted decimal 43
- downtime 118
- dropped 475
- dump 449
- duplex 475
- dynamic
 - IP 332
 - URL 110

E

- ECHO_REQUEST 118, 119, 241
- ECHO_RESPONSE 119
- EFI 131, 132

- element
 - XML 392, 408
- _email 43
- email
 - address 131, 132
 - alerts 72
 - reports 72
- encoding 52, 209
- encryption
 - backup 186
 - HTTP request 140
- error
 - ambiguous 51
 - CLI 38, 39, 40, 51
 - invalid object 40
 - page 117
 - syntax 320
 - XSS 51
- escape codes 133
- Ethernet 36, 37, 38, 134, 475, 489
- frame 225
- event
 - log 365
- Exchange Server 2003 261, 263
- execute 507
- expected input
 - CLI 25, 38

F

- fail-open 204
- failover 218
 - unintentional 218
- fail-to-wire 204
- failure
 - hardware 474
 - link 501
 - PSU 204
 - resilience 218
- false positive 65, 284, 315
- fault tolerance 204, 213
- field 40
- file
 - compress 288
 - size limit 296
 - system 504
 - system check 468
 - type 288, 289, 297
 - antivirus 178
 - report 86
 - uncompress 290
 - upload restriction 292, 295
- fingerprint 37
- FIPS-CC 37
- firewall
 - generic 337
- firmware
 - installing 530
 - partition 500
 - restoring 34, 530

- flag 489
- Flash 297, 355, 392, 408
- flash 500
- flood
 - HTTP request 324
 - SYN 203
 - TCP connection 313
- flow
 - control 35
 - packet 455
- forensic analysis 65
- format log disk 516
- fortianalyzer-policy 80
- FortiGate 101, 228
- FortiGuard
 - IP Reputation 332
- Fortinet
 - customer service 23
 - Distribution Network (FDN) 181, 429
 - Technical Documentation
 - conventions 23
 - Technical Support 489
- _fortinet_waf_auth 393
- FortiWeb
 - 1000C 204, 468
 - 3000C 204
 - 3000CFsx 204
 - 3000D 468, 504
 - 3000DFsx 204
 - 4000C 204
- FortiWeb-VM 213, 465, 466
- _fqdn 43
- fragment 489
- frame 475
- FTP 135
 - allowing through 101
 - backup via 187
 - server, upload debug logs to 464
- fully qualified domain name (FQDN) 43

G

- gateway 230
 - router 103
- GB2312 53
- geography 299
- GET 120, 146
- get 167
- grade point average (GPA) 131, 132
- gratuitous ARP 216
- greedy 68
- group
 - admin 243
 - ID (HA) 502
 - LDAP 246
 - user 254

H

- handshake 177
- hardening security 167, 319

- hardware 466
 - failure 118, 213, 474, 501
 - physical 469
 - specifications 474
 - virtual 465, 466, 469, 474
- hash 210, 497
- hasyncd 430, 506
- hatakd 433, 506
- HEAD 146
- header
 - IP 227
- health check
 - server 118
- heartbeat 236
 - HA 217
- hexadecimal 133, 134, 489, 501
- high availability (HA) 213
 - configuration synchronization without 198
 - heartbeat interface 215
 - main 213
 - mode 214
 - monitoring failovers via SNMP 236
 - standby appliance 213
 - VMware 213
- Host 105
- host
 - name
 - FortiWeb 206, 208
 - web server 380
 - protected 105
 - web 380
- Host: 105, 106, 143, 176, 316, 366, 380, 385, 386
 - allowed 105
 - rewrite 380
- HSTS 148, 160
- HTTP 118, 222, 223
 - 1.1 146
 - authentication 249, 251, 254, 307, 310
 - CONNECT 183
 - content routing 143
 - GET 120
 - header 105
 - parser 66, 146, 458
 - POST
 - antivirus scan 178
 - XML 392, 408
 - request
 - rate 324, 339
 - session 396
 - timeout 119
- HTTPS 194, 222, 223
 - service 148
 - timeout 119
- httpsd 506
- hypertext markup language (HTML) 133
- hypervisor 213

- I
- ICMP 119, 241
 - ECHO_REQUEST 118, 119
 - ECHO_RESPONSE 222, 223, 242
 - type 0 119
 - type 8 119
- ID
 - 70007 336
 - called station 253
 - field in IP header 177
 - file type 297
 - globally unique (GUID) 131, 132
 - HA group 214
 - Kuwaiti Civil 133
 - packet 489
 - process 498
 - session 396
 - signature 359
 - Social Security 135
 - uniform resource (URI) 135
 - user 495
 - VLAN 225
- idle
 - CPU 545
- IEEE
 - 802.1d 241
 - 802.1q 225
- incomplete command 39
- indentation 40
- _index 43
- index number 43
- information disclosure 355
- initialization
 - vector 177
- Inline Protection mode 225
- input
 - /output (I/O) 469
 - CLI 51
 - constraint
 - CLI 25, 38
 - web application 327
 - invalid 40
 - method 53
 - web page 327
- _int 43
- interface address
 - resetting 515
- Internet Explorer 6 208
- interrupt (IRQ) 469, 474, 475
- interval
 - alert email 64
 - anti-defacement monitoring 256
 - ARP 216
 - HA heartbeat 217
 - health check 119
 - NTP 211
 - web UI widget refresh 210
- inter-VLAN routing 225

IP

- address 224, 236
 - private network 24
- blacklist 336, 337
- forwarding 101
- list policy 336
- reputation intelligence 332
- trusted 336, 337
- v6 224
- virtual (VIP) 101, 105
- _ipv4 43
- _ipv4/mask 43
- _ipv4mask 43
- _ipv6 43
- _ipv6mask 43
- ISO 8859-1 53

J

- Java server pages (JSP)
 - adjusting auto-learning for 112
- JavaScript 302, 544
- jitter 221
- Joomla 285
- JPG 297

K

- keep-alive 146
- key
 - HTTP header 276
 - private 185, 186, 508, 510
 - product activation 133
 - SSH 37
 - strength 211

L

- language 52, 53, 206, 209
 - web UI 209
- Layer
 - 1 489, 501
 - 2 215, 225, 231, 241
 - 3 121, 225
 - 4 121
 - 6 158
 - routing 121
- LDAP
 - bind 247
 - password 247
 - query 245
- LDAPS 247
- limit
 - file size 296
 - rate 324, 339
- line endings 55

link 218

- detected 474
- encapsulation 475
- failure 218
- HA 434, 501
- layer 489
- mode 475
- monitor 218
- pair 204
- status 474, 501
- listening port number 206
 - web proxy 183
- load
 - balancer 143, 451
 - CPU 236, 505, 545
 - process 545
 - RAM 506, 545
- load balancer 415
- local
 - console access 34
 - domain name 201
- locale 53
- location 382
- Location: 384
- log
 - attack 284, 334, 337, 359, 375
 - attacks 275, 283, 304, 314, 322, 325, 328, 333, 340, 343, 358, 365, 369, 393, 394, 408
 - debug 424
 - mount point 504
 - severity 284, 334, 337, 359, 375
- login 249, 253
 - administrator 171, 249
 - failed 365
 - successful 365
 - user 365
- login prompt 35
- loop
 - Layer 2 241
 - redirect 398
- loopback 134, 474, 481, 483
- low encryption (LENC) 37

M

- mailto 135
- main 213
- maintenance 213
- malformed request 320
- management information block (MIB) 234, 239
- man-in-the-middle (MITM) 177
- markup 133
- master 213
- maximum transmission unit (MTU) 225, 475
- MD5 210, 433
- media access control (MAC) address 241
 - virtual 214, 216, 501
- memory
 - cache 472
 - usage 236, 471, 497, 498, 505, 545

- messages
 - log 365, 392, 408
- metric 475
- Microsoft
 - activation key 133
 - Active Directory 251, 363
 - Exchange Server 2003 261, 263
 - Internet Explorer 6 208
 - Office 297
 - Outlook Web App 110
 - Outlook Web App (OWA) 112
 - Outlook Web Application (OWA) 364
 - SharePoint 364
 - Threat Management Gateway 364
- miglogd 436, 506
- MIME 385
- minimum cost path 241
- mode
 - high availability (HA) 214
 - inline protection 225
 - offline protection 230
 - reverse proxy 230
 - transparent inspection 225, 231
 - true transparent proxy 204, 225, 230
- monitord 506
- more 54, 200
- mount 504
- MP3 297
- MPEG 297
- multicast 215
- multi-line command 39, 51
- multiple pages 200
- multiplexing 148

N

- _name 43
- National Insurance Number (NINO) 133
- negotiation 175
- nested compression 178
- netmask 172, 173, 224
 - administrator account 172, 173
- network
 - address translation (NAT) 270, 313, 337, 414, 451
 - source (SNAT) 228
 - interface
 - card (NIC) 474
 - SNMP monitoring 236
 - private 105
 - route 483
 - time protocol (NTP) 210
 - topology 213
- next-hop router 103
- no object in the end 39
- NT LAN Manager (NTLM) 251
- NTP
 - synchronization 206
- null modem 34, 36

O

- object 38, 39
- offline protection mode 230
- offloading
 - compression 288
 - SSL 194
 - TLS 194
- one-arm 165
- Online Certificate Status Protocol (OCSP) 150, 196
- operation mode 140, 230
 - number 499
 - switching 230
- operator 38
 - error 40
- option 40
- Outlook Web App (OWA) 110

P

- packet
 - capture 487
 - dropped 454, 475
 - payload 65, 97
 - trace 65, 487
- paging 200
- parameter
 - in URL 317
 - structure 110
 - value 114
- parity 35
- parser 435
 - buffer 66
 - error 51, 459
 - HTTP 146, 458
 - HTTP protocol 66
 - XHTML 392, 408
 - XML 392, 408
- partition
 - firmware 500
- password 35, 172
 - administrator 23
 - backup
 - encryption 186
 - FTP 186
 - LDAP bind 247
 - lost 49, 171
 - reset 49
 - strong 133, 211
 - weak 133
 - web proxy 183
- _pattern 43
- pattern
 - execute ping-options 525, 527
 - regular expression 43
- payload
 - content 319
 - packet 65
- PCI DSS
 - contraindications 210, 211
- PDF 297
- peer connection 35

- performance 24, 118, 125, 241, 336
 - and buffer size 176
 - antivirus 178
 - compression 175, 176
 - debug logs 424
 - HA 520
 - packet capture 487
 - response cache 175
 - rewriting 175, 176
 - system 505
 - TCP connection recycling 228
 - TCP timestamp and RTO 228
- period block 275, 283, 293, 304, 314, 322, 325, 328, 333, 340, 343, 358, 369, 393, 394, 408
- permissions 47, 49, 167, 171
 - account 167
- phishing 332
- phone number 134
- ping 118, 222, 223, 241, 242
 - timeout 119
- plain text editor 55
- policy
 - and operation mode 140
 - IP list 336
 - server 140
 - SNMP monitoring 236
 - trigger 284, 334, 337, 376
 - URL rewriting 380
- port
 - Ethernet 474
 - number 147, 148, 489, 497
- port1 543
- port2 543
- port3 204, 543
- port4 204
- port5 204
- port6 204
- port7 204
- port8 204
- POST 392, 408
- postal code
 - Canadian 131, 132
 - Chinese 131, 132
 - Danish 131, 132
 - Dutch 133
 - Quebec 134
 - Sweden 134
 - UK 134
 - USA 135
- postnummer 134
- power
 - interruption 204
 - loss 204
 - supply unit (PSU) 204

- predefined
 - attack signature 181
 - data type 130, 131, 132, 181
 - network service 163
 - robot 181
 - sensitive data in logs 67
 - suspicious URL 127, 181
- primary
 - appliance 213
 - DNS server 201
 - heartbeat interface 215
- priority
 - device 434
 - HA 214
 - route 483
- private
 - key 185, 186, 508, 510
 - network address 105
- process
 - load 545
- process ID (PID) 498, 503
- PROPFIND 261, 263
- protocol 489
- proxy 414, 415
 - anonymizing 332
 - HTTP 146
 - processes 545
 - reverse 230
 - server 183
 - transparent 230
 - web 183, 451
 - XML 438

Q

- query
 - anonymous 246
 - DNS 201
 - filter 246
 - LDAP 246
 - RADIUS 252
 - reverse DNS 376
- queue 475, 497

R

- radius-user 252
- RAID 477
- RAM
 - usage 506, 545
- Range: 317, 321
- rapid spanning tree protocol (RTSP) 241
- rate limit 273, 324, 339
- RC4 177
- reachable 103
- read-only 47
- reboot 204
- recursive
 - compression 178
 - URL encoding 175

- redirect 380, 382
 - attack 283, 304, 328, 333, 359, 369
 - loop 398
 - rewrite 380
- redundancy 213, 215
- Referer: 176, 380, 384, 385, 386
 - rewrite 380
- reformat disk 516
- regular expression 43, 65, 67, 113, 135, 261, 277, 284, 296, 329, 351, 360, 366, 370, 376, 386
- regular expressions 55
- remote file inclusion (RFI) 355
- repeat-count
 - execute ping-options 525, 527
- report
 - on demand 83
 - periodically generated 83
- reset 230
 - connection 275, 283, 293, 304, 322, 325, 328, 333, 340, 358, 369, 375, 394
 - from port 144
 - degug settings 463
 - password 49, 171
- restoring the firmware 34
- retry
 - health check 119
- reverse proxy 225, 230
 - mode 230
- rewrite
 - body 380
 - Host: 380
 - redirect 380
 - Referer: 380
 - URL 380
- RFC
 - 1918 24
 - 2518 261, 263
 - 2548 171, 252, 253
 - 2616 183, 385
 - 3849 24
 - 5246 175
 - 5737 24
 - 6176 210, 211
 - 6797 148, 160
 - 792 119
- RJ-45 36
- RJ-45-to-DB-9 34, 36
- robot 397, 410
- role
 - administrator 167
 - based access control (RBAC) 167
 - HA 502
- root 49
 - account 167
 - ADOM 60
 - CA 159

- route
 - cache 485
 - default 103
 - HTTP 158
 - Layer 6 158
 - static 103
 - table 483
- RST 230
- RTF bookmarks 133
- Rx 497
- S**
- schedule
 - report 83
- schema
 - directory 246
 - LDAP 246
- secondary
 - appliance 213
 - heartbeat interface 215
- Secure Shell (SSH) 34, 35, 36, 37, 222, 223
 - key 37
 - version 37
- security
 - known attacks 355
- segmentation fault 449
- sensitive information 355
- serial communications (COM) port 34, 35, 36
- serial number 502, 546
- server
 - health check 118
 - status 118
- service level agreement (SLA) 213
- session
 - administrative 544
 - IP 221
 - management 396
 - timeout 147, 396, 410
- Session-Id 409
- severity
 - level 284, 334, 337, 359, 375, 424
- SFTP
 - backup via 187
- SHA-1 37, 210
- shared Internet connection 227
- shared memory 471
- Shift-JIS 52, 53
- show 167, 547
- signature
 - attack 282, 355
 - data leak 282
 - virus 178
- signing chain 145, 159
- simple network management protocol (SNMP) 222,

- 223, 234
- change of IP address 236
- configuring community 234
- event 236
- manager 234, 239
- policy change monitoring 236
- system name 208
- trap 236
- single sign-on (SSO) 363
- slave 213
- sniffer 487
- SOAP 162
- Social Insurance Number (SIN) 131, 132
- Social Security Number (SSN) 134, 135
- socket 497
- sort code 134
- source
 - execute ping-options 525, 527
 - NAT 228
- spam 332
- spanning tree protocol (STP) 241
- special characters 52
- spider 397, 410
- SQL
 - injection 181, 355, 392, 408
 - statements 133
- SSH
 - allowing through 101
- SSL 160, 194, 247
 - certificate 144, 157
 - offloading 441
 - on the web servers 232
- SSL v2 support 209, 211
- SSL v3 support 176
- standalone 214
- standby 213
- STARTTLS 247
- state name 135
- static
 - route 103
 - URL 110
- status
 - server 118
- _str 43
- strength
 - encryption 211
 - key 211
 - password 133, 211
- strict transport security 148, 160
- string 43
- sub-command 39, 40, 44
- subnet 224
- swap 471, 545
- Swedish personnummer 134
- switch 213, 218
- SYN 119
 - flood 203
- synchronize 198, 210, 215

- syntax 25, 38
 - error 320
- Syslog 95
- T**
- table 39
- TCP 118, 443, 495
 - ACK 119
 - connection limit 313
 - flood 342
 - retransmission 221
 - retransmission timeout (RTO) 228
 - round trip time (RTT) 228
 - RST 144, 275, 283, 293, 304, 322, 325, 328, 333, 340, 358, 369, 375, 394
 - session timeout 147
 - SYN 119
 - flood 203
 - timeout 119
 - timestamp 228
- tcpdump 488
- technical support 23
- Telnet 34, 35, 36, 38, 222, 223, 534, 535
- throughput 498
- time 210, 513
 - daylight savings 207
 - in HTTP requests 131, 132
 - report 83
 - to live (TTL) 489
 - zone 206
- timeout 147, 497
 - authentication query connection 308
 - execute ping-options 525, 527
 - health check 118, 119
 - TCP retransmission 228
 - TCP session 147
- timestamp 448
 - TCP 228
- tips 24, 50
- TLS 160
 - offloading 441
- top processes 505
- tos
 - execute ping-options 525, 527
- trace 455, 487
- traffic 498
- transactions
 - accelerated by pipelining 146
- transparent
 - inspection mode 231
 - mode 220, 225
 - proxy 230
- traps 234
- trigger
 - policy 284, 334, 337, 376
- trojan 178
- troubleshooting 24, 423, 489
 - auto-learning 110
- true transparent proxy mode 204, 230
- True-Client-IP: 414

- trusted
 - host 172, 173
 - IP 336, 337
- ttl
 - execute ping-options 526, 527
- tunnel 183
- Tx 497
- type
 - 0, ICMP 119
 - 8, ICMP 119
 - file 288, 289
 - of service (TOS) bits 489, 525, 527

U

- UDP 497
- UK vehicle registration 134
- uncompress files 290
 - exception 286
- Unicode 52
- uniform resource identifier (URI) 135
- unknown action 39
- updated 506
- uptime 213, 506, 545
- URL
 - dynamic 110
 - encoding 175
 - interpreter 111
 - rewrite 379, 380
 - rewriting 380
 - static 110
- _url 43
- usage
 - bandwidth 498
 - CPU 236, 466, 505, 545
 - memory 545
 - RAM 471, 495, 497, 498
- US-ASCII 52, 53, 208, 489, 491
- user
 - name 171, 249
 - FTP 186
- user authentication
 - supporting modes 230, 231
- User-Agent: 176
- UTF-8 52, 209

V

- _v4mask 43
- _v6mask 43
- validate-reply
 - execute ping-options 526, 527
- value 40
 - parse error 40, 43
- VBScript 133
- vCPU 465, 466
- vDisk 473
- view-settings
 - execute ping-options 526, 527

- virtual
 - hardware 465, 466
 - IP (VIP) 101, 105
 - LAN (VLAN) 225, 483
 - trunk 225
 - MAC address 214, 216, 501
 - network interface 241, 481
 - server 151, 481, 543
 - VLAN (VLAN) 220
- vMotion 213
- vNIC 474
- vRAM 471
- vSwitch 241
- V-zone
 - and fail-to-wire 204

W

- W3C
 - HTML 133
 - XML
 - validation 392, 408
- web
 - proxy 183, 451
- Web 2.0 392, 408
- web crawler 397, 410
- web UI
 - language 209
- web vulnerability scan
 - policy 417
 - profile 419
 - schedule 421
- WebDAV 261, 263
- white list 125
 - IP 337
- wiki code 133
- wild cards 43
- WordPress 380
- wvs
 - policy 417
 - schedule 421
- WWW-Authenticate: 363

X

- X-Client-Cert: 144, 158
- X-Forwarded-For 413
- X-Forwarded-For: 413, 414, 415
- XHTML 392, 408
- XML 319
 - AJAX 392, 408
 - element 392, 408
 - malformed 392, 408
 - Microsoft Office 297
 - parser 392, 408
 - protection 392, 408
 - scanning 355
 - validate 392, 408
 - zip-compressed 297
- xmlproxy 506
- X-Real-IP: 413, 415

XSS 355

Z

ZIP

code 131, 132, 135
file 297

